ESCUELA DE ADMINISTRACIÓN DE NEGOCIOS – EAN

ANÁLISIS DE LA EJECUCIÓN Y CUMPLIMIENTO NORMATIVO DE LAS POLÍTICAS DE CIBERSEGURIDAD EN LA EDUCACIÓN PÚBLICA Y PRIVADA EN BOGOTÁ, 2010-2025

TESIS DE GRADO

ALAN GABRIEL VEGA TINJACÁ

NOVIEMBRE 20, 2025

Identificación del uso de la política pública y su efectivo cumplimiento en un entorno académico donde se sobrepone la ciberseguridad en la educación secundaria de carácter público y privado en Bogotá entre el periodo 2010-2025.

ANÁLISIS DE LA EJECUCIÓN Y CUMPLIMIENTO NORMATIVO DE LAS POLÍTICAS DE CIBERSEGURIDAD EN LA EDUCACIÓN PÚBLICA Y PRIVADA EN BOGOTÁ, 2010-2025

ALAN GABRIEL VEGA TINJACÁ

ESCUELA DE ADMINISTRACIÓN DE NEGOCIOS

EAN

FACULTAD DE INGENIERÍA

BOGOTÁ D.C. 2025

ANÁLISIS DE LA EJECUCIÓN Y CUMPLIMIENTO NORMATIVO DE LAS POLÍTICAS DE CIBERSEGURIDAD EN LA EDUCACIÓN PÚBLICA Y PRIVADA EN BOGOTÁ, 2010-2025

CLASIFICACIÓN: ACM CCS, IEEE Taxonomy

ALAN GABRIEL VEGA TINJACÁ

Tesis de grado para obtención del título de:

INGENIERO DE SISTEMAS

Director(a):

LEIDY NATALIA RESTREPO ZAPATA

ESCUELA DE ADMINISTRACIÓN DE NEGOCIOS

EAN

FACULTAD DE INGENIERÍA

BOGOTÁ D.C. DE 2025

AGRADECIMIENTOS

En este espacio agradezco a mi hermano mayor David Vega, por su esfuerzo y paciencia en lograr ser exitoso en todos los desafíos propuesto. En apoyo de mi tutora Leidy Restrepo y la intervención de los maestros a lo largo de estos 4 años, les doy las gracias por su apoyo a nosotros los estudiantes virtuales, estoy realizando mis estudios desde Chicago, IL. Otro país y me siento agradecido de tener la oportunidad de hacer parte de esta maravillosa universidad. Gracias a mi familia y compañeros académicos.

ANÁLISIS DE LA EJECUCIÓN Y CUMPLIMIENTO NORMATIVO DE LAS POLÍTICAS DE CIBERSEGURIDAD EN LA EDUCACIÓN PÚBLICA Y PRIVADA EN BOGOTÁ, 2010-2025

Este trabajo analiza la ejecución y cumplimiento normativo de las políticas de ciberseguridad en instituciones educativas públicas y privadas de Bogotá entre 2010 y 2025. Se examinan los marcos legales, normativos y técnicos, así como su implementación en colegios, identificando fortalezas, limitaciones y niveles de cumplimiento. A través de un enfoque combinado, se busca comprender el grado de preparación de las instituciones frente a riesgos digitales y proponer estrategias que fortalezcan la protección de datos y la seguridad en entornos educativos.

CLASIFICACIÓN: ACM CCS, IEEE Taxonomy

CONTENIDO

RESUMEN

La investigación examina el nivel de aplicación y cumplimiento de las políticas de ciberseguridad en instituciones educativas públicas y privadas localizadas en Bogotá, desde 2010 hasta 2025. Se utilizó una matriz de análisis documental, fundamentada en las directrices del MinTIC y el NIST, así como en la normativa nacional actual, utilizando un método no experimental, descriptivo y cuantitativo. La muestra estuvo compuesta por seis instituciones (tres privadas y tres públicas) en las que se examinaron aspectos como la infraestructura tecnológica, las políticas de seguridad, la capacitación del personal y la protección de datos. Los resultados muestran que hay una diferencia importante entre la existencia de políticas formales y su implementación real, lo cual es más notorio en las instituciones públicas. Se detectaron, además, diferencias entre las prácticas de las instituciones y los lineamientos regulatorios.

Basándose en los resultados, se sugieren soluciones estratégicas para reforzar el cumplimiento normativo. Se enfatizan medidas como la capacitación continua en ciberseguridad, la mejora de habilidades internas y el ajuste a normas internacionales. Esta tesis aporta elementos importantes para el diseño de políticas públicas más efectivas, sostenibles y acordes con las circunstancias del sector educativo colombiano. Además, colabora en la discusión técnica y académica acerca de la gobernanza digital a nivel escolar.

Palabras clave: Ciberseguridad, educación, políticas públicas, Bogotá, protección de datos, CONPES, ISO/IEC 27005, NIST SP 800-30., SANS Institute

ABSTRACT

This research examines the level of application and compliance with cybersecurity policies in public and private educational institutions located in Bogotá, Colombia, from 2010 to 2025. A document analysis matrix was used, based on guidelines from the Ministry of Information Technologies and Communications (MinTIC) and the National Institute of Standards and Technology (NIST), as well as current national regulations, employing a non-experimental, descriptive, and quantitative method. The sample consisted of six institutions (three private and three public) in which aspects such as technological infrastructure, security policies, staff training, and data protection were examined. The results show a significant gap between the existence of formal policies and their actual implementation, which is more pronounced in public institutions. Differences were also detected between the institutions' practices and regulatory guidelines.

Based on the results, strategic solutions are suggested to strengthen regulatory compliance. Measures such as continuous cybersecurity training, improvement of internal skills, and alignment with international standards are emphasized. This thesis contributes important elements to the design of more effective and sustainable public policies that are aligned with the circumstances of the Colombian education sector. Furthermore, it contributes to the technical and academic discussion on digital governance at the school level.

Keywords: Cybersecurity, education, public policies, Bogotá, data protection, CONPES, ISO/IEC 27005, NIST SP 800-30., SANS Institute

1. INTRODUCCIÓN

La transformación digital ha logrado atravesar con fuerza el sector educativo, impulsando procesos de virtualización, automatización y gestión de información a través de plataformas digitales. Aunque ofrece múltiples beneficios en términos de acceso, eficiencia y personalización del aprendizaje, también ha incrementado los riesgos asociados a la seguridad de la información, convirtiendo a las instituciones educativas en blancos crecientes de ciberataques. El uso de dispositivos personales, la interconexión en entornos colaborativos y la limitada inversión en infraestructura tecnológica han evidenciado vulnerabilidades críticas que afectan tanto a colegios públicos como privados.

En Colombia y especialmente en Bogotá, se han establecido marcos normativos relevantes orientados a regular la protección de datos, la ciberseguridad y la gestión del riesgo digital en el sector educativo. Sin embargo, la implementación efectiva de estas políticas aún enfrenta desafíos sustanciales, desde el desconocimiento institucional hasta las limitaciones presupuestales y técnicas. Esta situación plantea la necesidad de evaluar el grado de cumplimiento normativo, identificar brechas entre la regulación y la práctica, y proponer estrategias viables para cerrar dichas brechas.

La presente investigación tiene como propósito principal analizar la ejecución de políticas de ciberseguridad en instituciones educativas de Bogotá entre 2010 y 2025, comparando el cumplimiento normativo entre instituciones públicas y privadas. A través de un enfoque combinado, se pretende ofrecer evidencia empírica que sirva como base para la toma de decisiones, fortaleciendo así la protección de datos y la cultura de seguridad digital en el entorno escolar colombiano.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Analizar la implementación y el cumplimiento normativo de las políticas de ciberseguridad en instituciones educativas públicas y privadas de Bogotá durante el periodo 2010–2025, en el marco de la normativa nacional vigente.

2.2. OBJETIVOS ESPECIFICOS

1. **Identificar** el marco normativo, lineamientos y políticas vigentes en ciberseguridad aplicables al sector educativo en Bogotá.
2. **Describir** la situación actual de la ciberseguridad en las instituciones educativas publicas y privadas, identificando brechas de seguridad y riesgos predominantes a través del análisis de sus políticas institucionales.
3. **Comparar** lineamientos y recomendaciones dirigidas a las entidades reguladoras (MinTIC, Secretaría de Educación de Bogotá) y a los directivos de instituciones educativas públicas y privadas, orientadas a fortalecer la protección de datos personales, la gestión de riesgos y la cultura de **ciberseguridad** en el sector educativo
4. **Sugerir** lineamientos estratégicos para fortalecer el cumplimiento normativo de la ciberseguridad en el ámbito educativo de Bogotá, fundamentados en los hallazgos del análisis que permita cerrar las brechas cibernéticas en la educación y asegurar el cumplimiento efectivo de las normas vigentes de protección y seguridad de la información.

3. JUSTIFICACION

La **ciberseguridad** en Colombia se ha consolidado como un campo estratégico que articula dimensiones tecnológicas, jurídicas, educativas y sociales. El Proyecto de Ley 2023 sobre la Agencia Nacional de Seguridad Digital y Asuntos Espaciales la define como "la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales" (Congreso de la República de Colombia, 2023) Esta concepción sitúa a la **ciberseguridad** no solo como un conjunto de medidas técnicas, sino como un marco integral de protección que garantiza derechos fundamentales y la confianza en los entornos digitales.

En el caso del sector educativo, la importancia de la **ciberseguridad** se entrelaza con la protección de los datos personales. La Ley Estatutaria 1581 de 2012 establece el marco general para el tratamiento de datos en Colombia, otorgando especial protección a los niños, niñas y adolescentes, y determinando que el manejo de su información debe regirse por principios de legalidad, finalidad, seguridad y confidencialidad (Congreso de la República de Colombia, 2012). Estas disposiciones son de especial relevancia en Bogotá, donde la digitalización de la **educación** ha crecido exponencialmente.

El Estado colombiano ha acompañado este proceso mediante un marco normativo robusto. La Ley 1341 de 2009 y la Ley 1978 de 2019 sentaron las bases para la gobernanza de las TIC y la modernización del sector, promoviendo la conectividad y el acceso universal a servicios digitales seguros (Congreso de la República de Colombia, 2009; 2019) A nivel estratégico, documentos como el CONPES 3701 de 2011, el CONPES 3854 de

2016 y el CONPES 3995 de 2020 han delineado políticas públicas para fortalecer la **ciberseguridad** y la confianza digital en el país (Departamento Nacional de Planeación, 2011; 2016; 2020) Más recientemente, el Decreto 338 de 2022 estableció un modelo de gobernanza para la seguridad digital, evidenciando la necesidad de consolidar instituciones y lineamientos frente a amenazas crecientes en el ciberespacio (Ministerios de Tecnologías de la Información, 2022).

En el ámbito local, la Secretaría de Educación de Bogotá implementó el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (Secretaria de Educación de Colombia, 2020), que busca garantizar entornos educativos digitales seguros, inclusivos y confiables, reconociendo la **ciberseguridad** como un pilar de la calidad educativa (Departamento Nacional de Planeación, 2020). Estas políticas se alinean con marcos internacionales, como la (UNESCO, 2024), que enfatiza la necesidad de promover una **educación** digital que respete los derechos humanos, proteja la privacidad de los estudiantes y fomente la confianza en los ecosistemas tecnológicos.

Desde una perspectiva académica, autores como (Moreno, 2015) y (Gómez Rengifo, 2021) destacan que la **ciberseguridad** en Colombia debe ser concebida como un sistema integral de protección del ciberespacio, que combine medidas normativas, cooperación internacional y formación especializada. Estos enfoques son esenciales para comprender cómo las instituciones educativas pueden responder de manera efectiva a riesgos digitales y garantizar tanto la continuidad pedagógica como la protección de los datos de la comunidad académica. Más allá de la normativa local, marcos internacionales como **ISO**/IEC 27005:2022 y NIST SP 800-30 ofrecen guías técnicas para gestionar riesgos, mientras que el **SANS Institute** (Risto, 2023) y organismos como la (UNESCO, 2024) resaltan la

importancia de integrar la **ciberseguridad** en los sistemas educativos bajo principios de equidad, derechos humanos y confianza digital.

De esta manera, la presente investigación busca evaluar de qué manera las instituciones educativas públicas y privadas de Bogotá han incorporado las políticas nacionales, locales e internacionales de **ciberseguridad**, identificando avances, brechas y oportunidades de mejora. En este contexto, la presente investigación titulada "Análisis de la ejecución y cumplimiento normativo de las políticas de **ciberseguridad** en la **educación** pública y privada en Bogotá, 2010–2025" busca evaluar de qué manera las instituciones educativas han incorporado las políticas nacionales y locales de **ciberseguridad**, identificando avances, brechas y oportunidades de mejora. De este modo, se propone aportar a la construcción de un ecosistema educativo digital más seguro, resiliente y acorde con los retos de la transformación digital en Colombia

4. MARCO TEORICO

Para los propósitos de la investigación subsiguiente, definiremos el término ciberseguridad en términos generales y, en particular, en el contexto nacional e internacional. Según el proyecto de ley 2023 del Ministerio de Tecnologías de la Información y las Comunicaciones sobre la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, se puede entender como "la capacidad del Estado para disminuir el riesgo que corren sus ciudadanos frente a incidentes o amenazas cibernéticas, con el objetivo de garantizar la disponibilidad, autenticidad, confidencialidad, integridad y no repudio de las interacciones digitales". Esta definición se ajusta al objetivo de análisis del presente trabajo, ya que sitúa la ciberseguridad no solo como un proceso técnico, sino también normativo y estratégico. Este último está directamente relacionado con la protección de los datos ciudadanos en entornos altamente digitalizados, como el educativo.

En Bogotá, se ha observado que la digitalización de las instituciones educativas ha sido tan significativa que ha creado oportunidades para optimizar los procesos de gestión académica y enseñanza. Sin embargo, también ha puesto en riesgo a alumnos, educadores y familias en cuanto a la seguridad de datos personales y privacidad. Este desafío se vuelve relevante en el contexto de la Ley Estatutaria 1581 de 2012 (Congreso de la República de Colombia, 2012), que reconoce y regula el derecho básico de cada individuo a proteger sus datos, mediante la fijación de disposiciones generales para su recolección, tratamiento y circulación (Congreso de la República de Colombia, 2012).

En el marco colombiano, salvaguardar la información personal es uno de los fundamentos de la ciberseguridad. El derecho constitucional al hábeas data es desarrollado por la Ley Estatutaria 1581 de 2012, que también regula cómo se maneja la información en

bases de datos públicas y privadas. La ley establece principios como la legalidad, la finalidad, la libertad, la transparencia, la seguridad y la confidencialidad (Congreso de Colombia, 2012). Esta ley tiene una importancia particular en los contextos educativos, donde se manejan datos delicados de jóvenes y niños, y la protección es prioritaria y necesaria.

También la ciberseguridad nacional se basa en el marco legal de las telecomunicaciones y las TIC. La Ley 1341, promulgada en el año 2009, estableció los lineamientos para el progreso de la sociedad informativa en Colombia. Esta legislación incluyó principios de acceso y fomento a la inversión, así como de robustecimiento institucional (Congreso de la República de Colombia, 2009). Luego, la Ley 1978 de 2019 modificó el sector TIC. Se creó la Comisión de Regulación de Comunicaciones como autoridad única y se fortaleció el papel del Estado en asegurar tanto la seguridad digital como la conectividad (Congreso de la República de Colombia, 2019). Estas leyes son el fundamento para poner en práctica políticas de seguridad y confianza digital. En Colombia, los Decretos reglamentarios (el Decreto 2618 de 2012, el Decreto 1078 de 2015, el Decreto 1414 de 2017 y el Decreto 338 de 2022) han estado fortaleciendo la gobernanza del sector TIC y la seguridad digital al incorporar directrices para gestionar riesgos, estructurar la infraestructura crítica e implementar tácticas de gobierno digital (República de Colombia. Presidencia, 2012; 2015; 2017; 2022). Colombia ha progresado en términos de política pública mediante la emisión de documentos CONPES que definen directrices estratégicas. El CONPES 3701, emitido en 2011, estableció las primeras pautas relacionadas con la ciberdefensa y la ciberseguridad, destacando que era preciso robustecer las capacidades técnicas e institucionales para contrarrestar los peligros cibernéticos (Departamento

Nacional de Planeación, 2011). Después, el CONPES 3854 de 2016 dio a conocer la Política Nacional de Seguridad Digital, que incluye medidas para prevenir, detectar y administrar incidentes (Departamento Nacional de Planeación, 2016). El CONPES 3995 de 2020, más actualizado, consolidó la Política Nacional de Confianza y Seguridad Digital, que busca potenciar las habilidades de los ciudadanos, las empresas y las entidades públicas e impulsar la adopción de normas internacionales (Departamento Nacional de Planeación, 2020).

Con respecto a la educación, Bogotá ha puesto en marcha acciones concretas para adecuarla a la transformación digital. El Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2020-2024, diseñado por la Secretaría de Educación, establece medidas específicas para optimizar la seguridad digital y la infraestructura tecnológica en centros educativos públicos (Secretaría de Educación de Colombia, 2020). Además, la Ley 2294 del año 2023 y normativas anteriores como el Decreto 32 y la Ley 1623 de 2013 han fortalecido el deber del estado de asegurar ambientes digitales seguros en el sector educativo (República de Colombia, 2013; 2023).

Desde el punto de vista académico, tanto Gómez Rengifo (2021) como Moreno (2015) están de acuerdo en que la ciberseguridad debe ser entendida no solamente como un grupo de acciones técnicas, sino también como un sistema completo para proteger el ciberespacio. Este sistema necesita colaboración entre instituciones, inversión en capacitación y cooperación a nivel internacional, dado que las amenazas digitales van más allá de las fronteras. Gómez Rengifo (2021) subraya la habilidad del Estado para reaccionar de forma eficaz a los ciberataques, así como la importancia de la cooperación internacional. Moreno (2015), por su parte, destaca que es necesario incluir la ciberseguridad en el ámbito

de la defensa nacional. La UNESCO, entre otras entidades internacionales, subraya que la digitalización de la educación conlleva desafíos en términos de seguridad, sobre todo cuando se trata de proteger los datos personales de los niños y el empleo de plataformas digitales. Por lo tanto, se hace necesario crear políticas que aseguren ambientes digitales seguros, inclusivos y que respeten los derechos humanos (UNESCO, 2024).

En resumen, en Colombia la ciberseguridad es un entramado normativo y estratégico que combina leyes, decretos, políticas públicas y compromisos a nivel internacional. En lo que respecta a Bogotá y su sistema educativo, la aplicación de políticas de seguridad digital y la salvaguarda de los datos personales son factores esenciales para asegurar la continuidad de la transformación digital y también para mantener la confianza de los estudiantes, las familias y los maestros en el ecosistema educativo.

4.1. PANORAMA DE LA CIBERSEGURIDAD EN EL SECTOR EDUCATIVO

Para efectos de esta investigación, se adopta la definición de ciberseguridad propuesta en un reciente proyecto legislativo del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Dicho proyecto define la ciberseguridad como "la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales". Esta definición concibe la ciberseguridad como un proceso completo, que no es solo técnico sino también estratégico y normativo, relacionado directamente con la salvaguarda de los datos de las personas en contextos muy digitalizados, como el educativo.

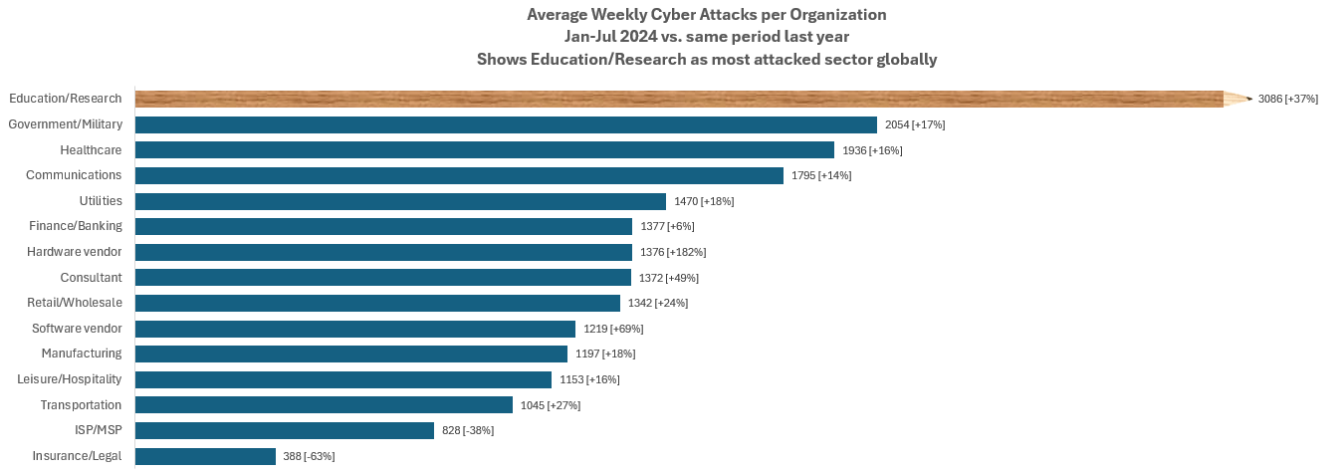
La rápida digitalización de las instituciones en el entorno educativo de Bogotá y Colombia ha ofrecido oportunidades para optimizar los procesos académicos y de

enseñanza. Sin embargo, también ha hecho que alumnos, maestros y familias enfrenten peligros asociados a la seguridad de la información y a la privacidad. Esto le da un particular significado a la Ley Estatutaria 1581 de 2012, también llamada Ley de Protección de Datos Personales, que reconoce y regula el derecho esencial de cada ciudadano a tener sus datos personales protegidos. La ley mencionada determina principios de confidencialidad, seguridad, transparencia, libertad, finalidad y legalidad en el manejo de datos; aspectos esenciales para contextos educativos que gestionan información delicada sobre menores. En conclusión, la protección de datos personales constituye uno de los fundamentos de la ciberseguridad educativa porque las instituciones educativas gestionan una cantidad significativa de información personal que necesita ser protegida.

A escala mundial y en Colombia, el sector educativo se ha vuelto uno de los más asediados por los cibercriminales. Según la información de Check Point Research, en Colombia el promedio semanal de ataques cibernéticos dirigidos a organizaciones educativas ha alcanzado los 8.959, lo que es más del doble que el promedio mundial, que es alrededor de 4.367 ataques semanales. La comparación se muestra en la figura 1, que destaca cuán grave es el escenario de amenazas en el sector educativo colombiano si se lo compara con la situación mundial. La alta tasa de ataques que se observa evidencia que las universidades y los colegios han pasado a ser un objetivo primordial, debido a la extensión de su superficie de ataque (cada vez más dispositivos conectados, servicios digitales y usuarios) y a una histórica ausencia de inversión en ciberseguridad, situación que los ciberdelincuentes explotan.

Ilustración 1. Comparación de los ataques cibernéticos semanales promedio en el sector educativo entre Colombia y el mundo (últimos seis meses de 2024).

Figura1. Average weekly cyber attacks per organization by sector (Jan–Jul 2024)



Nota. Adaptado de Check Point Research warns: Every day is a school day for cybercriminals with the education sector as the top target in 2024, por Check Point Research, 2024, Check Point Software Technologies (https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/):

De acuerdo con los datos de Check Point Research, una institución educativa en Colombia sufre semanalmente más del doble de ataques que la media mundial, según indican las cifras. Sobre estos riesgos en aumento en la educación digital, han alertado las organizaciones internacionales. La digitalización educativa, como señala la UNESCO, presenta desafíos significativos en materia de seguridad, sobre todo en lo que se refiere a la protección de datos de los menores y al uso de plataformas virtuales. Por lo tanto, es urgente crear políticas que aseguren ambientes de aprendizaje en línea que sean seguros, inclusivos y respeten los derechos humanos (UNESCO, 2024). Asimismo, los académicos expertos están de acuerdo en que la ciberseguridad no debe ser vista solo como acciones técnicas independientes, sino como un sistema integral de protección que incluye formación

constante, coordinación entre instituciones y hasta cooperación internacional (Moreno, 2015; Gómez Rengifo, 2021). En esta perspectiva, es necesario que las instituciones educativas fortalezcan sus habilidades tecnológicas (infraestructura, software de seguridad, etc.) y organizativas y humanas (políticas, protocolos, educación en ciberhigiene), teniendo en cuenta que los riesgos digitales van más allá de las fronteras y tienen el potencial de perjudicar seriamente la privacidad, la seguridad y el bienestar del conjunto educativo.

En síntesis, la ciberseguridad en entornos educativos implica **proteger la confidencialidad, integridad y disponibilidad** de los datos y sistemas escolares frente a un panorama de amenazas en constante evolución. Este concepto abarca aspectos legales (cumplimiento de normas de protección de datos y delitos informáticos), tecnológicos (uso de herramientas de seguridad) y de gestión (estrategias, planes y cultura institucional de seguridad). A continuación, se presenta el marco normativo que ha desarrollado Colombia para abordar estos retos, así como la evolución reciente de las políticas públicas relacionadas con la seguridad digital en la educación.

4.2. MARCO NORMATIVO DE LA CIBERSEGURIDAD EN COLOMBIA (2009-2025)

Colombia ha construido en las últimas dos décadas un entramado normativo robusto en materia de seguridad digital, con leyes, decretos y políticas públicas orientadas a fortalecer la confianza y seguridad en el ecosistema cibernético. A nivel nacional, este marco legal-normativo sienta las bases para la protección de datos personales, la seguridad de la información y la respuesta a incidentes cibernéticos, todo lo cual impacta directamente al sector educativo. En la Tabla 4.2.1 se presenta una cronología de las

principales normas y políticas nacionales en ciberseguridad entre 2009 y 2025, haciendo énfasis en aquellas de mayor relevancia para el ámbito educativo:

Año	Norma clave	Aspectos relevantes
2009	**Ley 1341 de 2009** (Ley TIC)	Establece el marco para el desarrollo de la sociedad de la información en Colombia, definiendo principios de acceso universal, promoción de la inversión y fortalecimiento institucional del sector TIC. Sienta bases para la masificación de Internet y servicios digitales, precondición para abordar la seguridad digital.
2011	**Documento CONPES 3701** – Lineamientos de Política en Ciberseguridad y Ciberdefensa	Primer documento de política pública en ciberseguridad. Subraya la necesidad de fortalecer capacidades institucionales y técnicas para enfrentar amenazas cibernéticas, incluyendo la creación de grupos de respuesta a incidentes y cooperación entre defensa, gobierno y sector privado.
2012	**Ley 1581 de 2012** (Ley de Protección de Datos Personales)	Desarrolla el derecho constitucional de *hábeas data*. Establece principios y disposiciones para la recolección, tratamiento y circulación de datos personales en bases de datos públicas y privadas, incluyendo obligaciones para instituciones educativas

		en cuanto al manejo seguro de datos de estudiantes y docentes.
2012	**Decreto 2618 de 2012**	Modifica la estructura del Ministerio TIC. Crea dependencias especializadas que consolidan la gobernanza de las TIC y, por ende, de la seguridad digital (por ejemplo, integró la seguridad de la información dentro de las funciones del Ministerio). Este decreto fortaleció la capacidad institucional para liderar iniciativas de seguridad cibernética a nivel nacional.
2013	**Ley 1620 de 2013** (Convivencia Escolar)	Crea el Sistema Nacional de Convivencia Escolar. Si bien su foco es la prevención del acoso y violencia escolar, incluye lineamientos para fomentar **ambientes escolares seguros**, lo cual abarca la prevención de riesgos en entornos digitales (p. ej., cyberbullying, protección de menores en Internet). Refuerza la obligación del Estado de garantizar entornos educativos libres de amenazas a la integridad de los estudiantes, incluyendo las de índole cibernética.
2013	**Decreto 32 de 2013**	Crea la *Comisión Nacional Digital y de Información del Estado* para la seguridad cibernética. Esta comisión intersectorial tuvo como objeto coordinar la

		atención de incidentes de **ciberseguridad y ciberdefensa** a nivel nacional, integrando entidades del gobierno en la gestión de riesgos digitales. Fue un paso inicial en la organización gubernamental frente a amenazas cibernéticas emergentes. *(Nota: Derogada posteriormente por el Decreto 611 de 2018)*.
2015	**Decreto 1078 de 2015** (Decreto Único TIC)	Compila y actualiza toda la normativa del sector TIC en un solo cuerpo. Incluye disposiciones sobre **gobierno digital** y estándares de **seguridad de la información** para entidades públicas. Este decreto unificado facilitó la aplicación consistente de lineamientos de seguridad digital en todo el Estado, incluyendo el sector educativo público.
2016	**Documento CONPES 3854 de 2016** – Política Nacional de Seguridad Digital	Establece la primera Política Nacional de Seguridad Digital. Articula acciones de **prevención, detección, respuesta y recuperación** ante incidentes cibernéticos. Plantea programas de concientización, creación de equipos de respuesta a incidentes (CSIRTs), protección de infraestructuras críticas y desarrollo de marcos de seguridad en entidades públicas. Este CONPES marcó un hito al definir una estrategia integral de seguridad digital en Colombia.

2017	**Decreto 1414 de 2017**	Fortalece la institucionalidad en seguridad digital. Ajusta la estructura del Ministerio TIC y otras entidades para mejorar la **gestión del riesgo cibernético** y la **respuesta a incidentes** (por ejemplo, consolidó el Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT). En línea con la Política de 2016, este decreto buscó cerrar brechas organizacionales en ciberseguridad dentro del Estado.
2018	**Decreto 611 de 2018**	Reorganiza la gobernabilidad de la seguridad en el ámbito digital. Eliminando la Comisión Nacional Digital, establecida en 2013, y traspasando sus responsabilidades a estructuras de coordinación más modernas (por ejemplo, el Comité de Seguridad Digital del país). Esto facilitó la organización de las instituciones, eliminando duplicaciones y sincronizando la coordinación de sucesos con la reciente política nacional.
2019	**Ley 1978 de 2019** (Modernización del sector TIC)	Modifica el marco de las TIC en Colombia. Promueve la inversión en conectividad y establece un regulador convergente único (Comisión de Regulación de Comunicaciones - CRC). Contiene órdenes para aumentar la seguridad de las redes y salvaguardar a los usuarios en servicios digitales. Fortalece la función del

		Estado de asegurar un entorno digital de confianza, que es el fundamento para elaborar estrategias de ciberseguridad.
2020	**Documento CONPES 3995 de 2020** – Política Nacional de Confianza y Seguridad Digital	Concentrándose en mejorar las habilidades de ciberresiliencia del país, actualiza la política nacional de seguridad digital. Establece metas para el 2025 en tres áreas: (1) Potenciar las habilidades nacionales (desarrollo de talento, investigación y desarrollo en ciberseguridad), (2) salvaguarda de infraestructuras críticas y (3) promoción de la confianza digital (marcos normativos, estándares globales, cooperación entre el sector público y privado). Este documento orienta las estrategias más recientes, de acuerdo con tendencias emergentes como la digitalización acelerada y la inteligencia artificial.
2020	**Decreto 1064 de 2020**	Para fortalecer la seguridad digital, cambia la estructura interna del MinTIC. Establece dependencias como la Dirección de Seguridad Digital, que tiene la responsabilidad de inspeccionar, vigilar y controlar los temas relacionados con la seguridad de los datos y los servicios digitales para ciudadanos. En resumen, incluye de manera más explícita la seguridad

		cibernética en las funciones orgánicas del Ministerio, garantizando un liderazgo claro en este campo.
2021	**Ley 2170 de 2021** (Uso de tecnologías en educación)	Para fortalecer la seguridad digital, cambia la estructura interna del MinTIC. Establece dependencias como la Dirección de Seguridad Digital, que tiene la responsabilidad de inspeccionar, vigilar y controlar los temas relacionados con la seguridad de los datos y los servicios digitales para ciudadanos. En resumen, incluye de manera más explícita la seguridad cibernética en las funciones orgánicas del Ministerio, garantizando un liderazgo claro en este campo.
2022	**Decreto 338 de 2022**	Para fortalecer la seguridad digital, cambia la estructura interna del MinTIC. Establece dependencias como la Dirección de Seguridad Digital, que tiene la responsabilidad de inspeccionar, vigilar y controlar los temas relacionados con la seguridad de los datos y los servicios digitales para ciudadanos. En resumen, incluye de manera más explícita la seguridad cibernética en las funciones orgánicas del Ministerio, garantizando un liderazgo claro en este campo.
2023	**Ley 2294 de 2023** (Creación de la Agencia	Establece la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, organismo que tiene como

	Nacional de Seguridad Digital)	responsabilidad la coordinación para poner en marcha políticas de seguridad digital, manejar amenazas cibernéticas y reaccionar ante incidentes a nivel nacional. Colombia, con esta legislación, da un paso importante en cuanto a instituciones al crear una entidad dedicada a la ciberseguridad, la cual está en línea con las normas internacionales y tiene el poder de coordinar esfuerzos entre diferentes sectores. La agencia posibilitará la implementación de estrategias de seguridad digital en áreas como la educación, garantizando que las reglas se cumplan efectivamente y que haya una respuesta adecuada frente a incidentes de ciberseguridad.
2025	**Estrategia Nacional de Seguridad Digital 2025–2027** (MinTIC, 2025)	Lanzada en junio de 2025 como una actualización de la política nacional (CONPES 3995). Destaca la capacidad de recuperación cibernética a nivel nacional frente a amenazas complejas potenciadas por la inteligencia artificial. Se estructura en tres pilares: (1) Competencias nacionales (que incluye el objetivo de crear 10.000 nuevos expertos en datos, inteligencia artificial y ciberseguridad para el año 2026), (2) Salvaguarda de infraestructuras esenciales y (3) Confianza digital. Propone la formación de un Centro

		Nacional de Operaciones de Seguridad (SOC) y fortalece la colaboración entre el sector público y el privado. Esta hoja de ruta orienta acciones específicas para los años venideros, muchas de las cuales afectan la educación (por ejemplo, programas de capacitación en seguridad digital para alumnos y maestros).

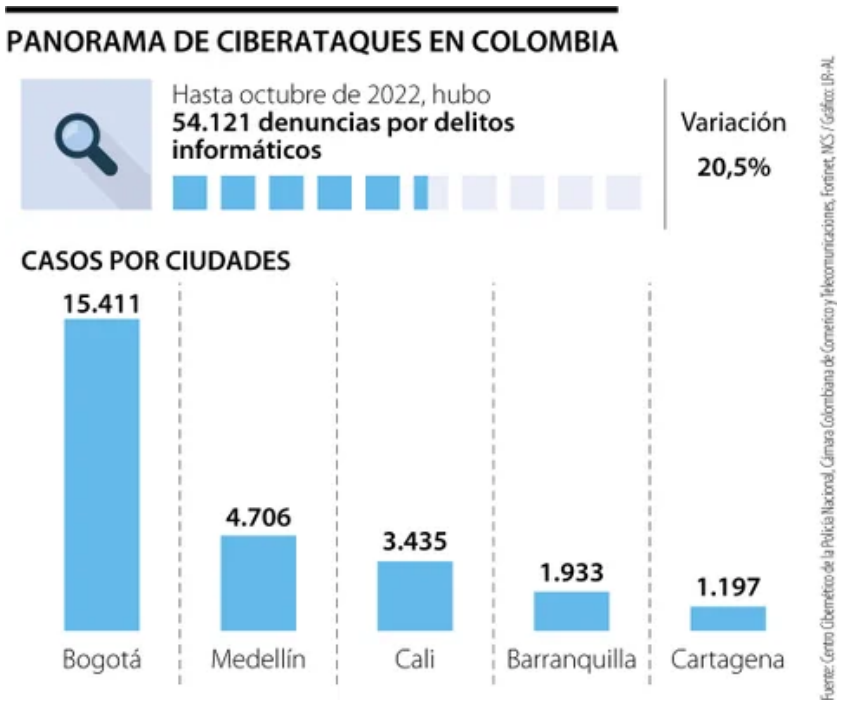
Tabla 4.2.1. Cronología de normativa nacional en materia de ciberseguridad (2009–2025)

Como se observa en la tabla, Colombia ha avanzado significativamente en la creación de un andamiaje legal e institucional para la ciberseguridad. Normas como la Ley 1341 (que impulsó la conectividad) y la Ley 1581 (que protege los datos personales) proveen fundamentos esenciales. A su vez, decretos ejecutivos han ido ajustando la estructura estatal para responder mejor a los retos digitales (por ejemplo, la creación de ColCERT, la definición de infraestructuras críticas cibernéticas, etc.). De especial importancia es la reciente Ley 2294 de 2023, que establece una Agencia Nacional de Seguridad Digital, indicando la prioridad que el tema ha cobrado en la agenda pública. Todo este marco normativo aplica transversalmente a múltiples sectores, incluyendo la educación. Las instituciones educativas, públicas y privadas, están sujetas a estas leyes y políticas: deben cumplir con estándares de protección de datos, implementar medidas de seguridad de la información, reportar incidentes al Centro Cibernético Policial o ColCERT, y en general alinear sus prácticas con la estrategia nacional de seguridad digital.

No obstante, a pesar de contar con un marco normativo amplio en materia de ciberseguridad, los incidentes cibernéticos continúan en aumento en Colombia, lo que evidencia desafíos persistentes en la implementación efectiva de dichas políticas. De

acuerdo con datos reportados por medios económicos y autoridades judiciales, hasta octubre de 2022 se registraron 54.121 denuncias por delitos informáticos, con una variación anual superior al 20%, concentrándose principalmente en ciudades como Bogotá, Medellín y Cali (La República, 2022). La Figura 4.2.1 presenta un panorama general de la distribución territorial de estos incidentes.

Figura 4.2.1: Panorama de ciberataques en Colombia por ciudades (2022)

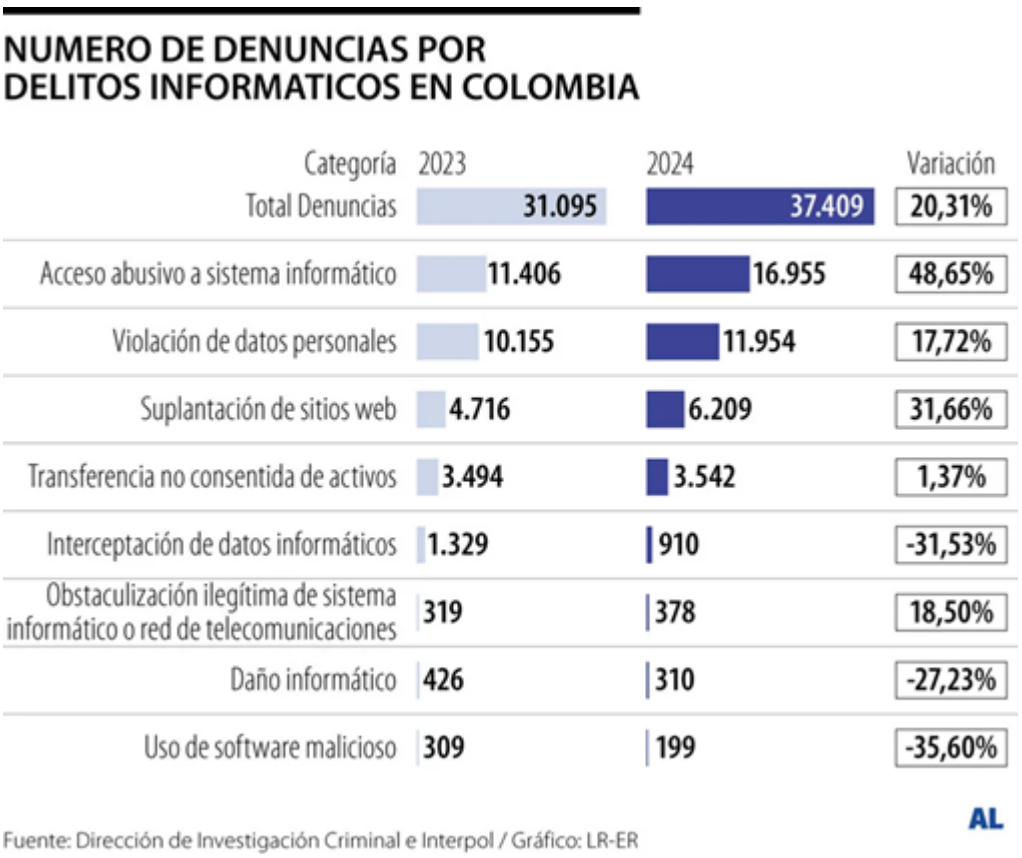


Nota. Reproducido de Los ciberataques suman 54.121 casos en lo que va del año y han crecido más de 20%, por La República, 2022.

En años recientes, esta tendencia no solo se ha mantenido, sino que se ha intensificado. Según información de la Dirección de Investigación Criminal e Interpol de la Policía Nacional, en 2023 se registraron 31.095 denuncias por delitos informáticos, mientras que en 2024 la cifra ascendió a 37.409, lo que representa un incremento del

20,31% en un solo año (Asuntos Legales, 2024). Esta evolución se ilustra en la Figura 4.2.2, que compara el total de denuncias registradas en ambos periodos.

Figura 4.2.2 Número de denuncias por delitos informáticos en Colombia (2023–2024)

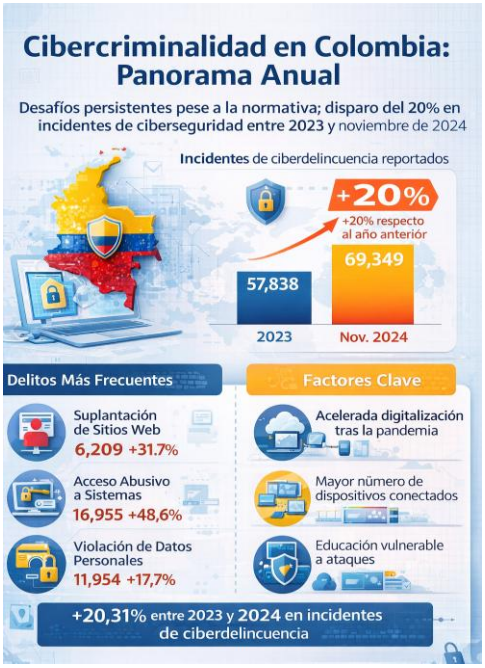


Nota. Reproducido de datos de la Dirección de Investigación Criminal e Interpol, citado en Asuntos Legales (2024).

Al analizar la tipología de delitos informáticos más frecuentes reportados en Colombia entre 2023 y 2024, se observa una coincidencia entre fuentes oficiales y análisis sectoriales. Según la Dirección de Investigación Criminal e Interpol, conductas como el acceso abusivo a sistemas informáticos, la suplantación de sitios web y la violación de datos personales concentraron un gran número de denuncias en este periodo. Este patrón

también es señalado por especialistas en ciberseguridad, quien destacan estos mismos delitos, junto con fraudes digitales y ataques de ingeniería social, como los riesgos más recurrentes en el país (Impacto TIC, 2025). La Figura 4.2.3 sintetiza estas categorías y su comportamiento relativo entre 2023 y 2024.

Figura 4.2.3 Delitos informáticos más frecuentes en Colombia (2023–2024)



Nota. Adaptado de Impacto TIC: Ciberseguridad en Colombia — riesgos, por Impacto TIC (2025), y datos de la Dirección de Investigación Criminal e Interpol (2024). Recuperado de https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-pais/

Este fenómeno no se limita al contexto nacional. En el ámbito regional, América Latina recibió más de 350.000 millones de intentos de ciberataques durante 2022, ubicando a Colombia entre los países más afectados, con aproximadamente 20.000 millones de

intentos registrados (Fortinet, 2022). La Figura 4.2.4 sitúa a Colombia dentro del panorama latinoamericano de amenazas cibernéticas, evidenciando la magnitud del desafío.

Figura 4.2.4 Países con mayor número de intentos de ciberataques en América Latina (2022)

Nota. Reproducido de Fortinet Threat Landscape Report, citado en La República (2022).

En resumen, Colombia ha creado un marco legal y estratégico extenso para la ciberseguridad que integra leyes, decretos, políticas del país e iniciativas de las instituciones. La implementación de este marco regulatorio es crucial para asegurar la seguridad de los datos personales de la comunidad académica y el sostenimiento del cambio digital en la educación en un ambiente confiable, especialmente en relación con

Bogotá y su sistema educativo. Que existan políticas es un paso esencial; sin embargo, el verdadero desafío es que se implementen de manera efectiva en colegios y universidades: esto conlleva proporcionar recursos a las instituciones, formar al personal, establecer protocolos claros y promover una cultura de ciberseguridad desde las aulas hasta los directivos. La única forma de cerrar la brecha en términos de ciberseguridad entre la educación pública y privada es a través de una combinación sólida del cumplimiento normativo y la práctica activa de seguridad digital. Esto garantizará entornos resilientes y seguros para el aprendizaje, capaces de resistir amenazas del mundo cibernético.

4.3. FALENCIAS ESTRUCTURALES EN EL CONTEXTO EDUCATIVO

Las falencias estructurales en el ámbito educativo se han puesto de manifiesto debido al rápido proceso de digitalización que ha tenido lugar en las escuelas; estas son las carencias propias de la infraestructura, los procesos y los recursos humanos de las instituciones educativas. En primer lugar, las instituciones administran información sensible de alumnos y familias (nombres, identificaciones, domicilios, datos de contacto, historiales) que los delincuentes cibernéticos buscan con gran interés. Si no se protege de manera apropiada, esta información hace que las escuelas sean objetivos atractivos. Los colegios, además, funcionan con varios puntos de acceso a sus redes: los estudiantes, los maestros, el personal administrativo, los padres y los proveedores se conectan a los sistemas institucionales a través de diferentes dispositivos (como tabletas, teléfonos inteligentes personales o computadoras escolares), muchos de ellos posiblemente sin monitoreo o sin medidas de seguridad actualizadas. Esta extensa superficie de ataque, con usuarios que acceden a la escuela tanto desde dentro como fuera las 24 horas del día y los siete días de la semana, incrementa las oportunidades de intrusiones y complica el control centralizado.

La falta de hardware y de medidas de seguridad en los perímetros escolares es otro elemento crucial. Por motivos de recursos limitados, la mayoría de las instituciones educativas

públicas no cuentan con sistemas especiales, como firewalls de alto rendimiento, sistemas para prevenir intrusos o esquemas sólidos para copias de seguridad. Hay algunas entidades privadas, en particular las más pequeñas, que no invierten en medidas de ciberseguridad avanzadas porque las consideran gastos innecesarios. En Colombia, la gran mayoría de las escuelas públicas de educación media y básica carecen de un Sistema de Gestión de Seguridad de la Información (SGSI) o personal especializado solo en seguridad digital. Esta falta de personal calificado que tenga dedicación exclusiva significa que la seguridad informática se deja en manos de empleados tecnológicos con muchas responsabilidades o incluso de maestros con conocimientos básicos en informática pero sin formación en ciberseguridad. Las disparidades en las prácticas y la cultura empeoran la situación. Investigaciones recientes apuntan que las instituciones educativas a menudo no implementan ni los controles básicos de seguridad. Por ejemplo, un diagnóstico a nivel nacional reveló que muchas escuelas han sido objeto de ataques a sus bases de datos y que en la mayoría de los casos esto ocurrió debido a la ausencia de medidas básicas de protección (uso de antivirus actualizados, realización periódica de copias de seguridad y configuración de cortafuegos).

Además, el factor humano continúa siendo un vector de riesgo significativo: tanto los alumnos como los profesores y el personal administrativo pueden ser blanco de ataques de phishing o fraudes de ingeniería social, lo que permite que se sustraigan credenciales e ingresos no autorizados. En realidad, se ha informado que solo un pequeño porcentaje de instituciones educativas implementa programas de concientización sobre seguridad para sus estudiantes en el ámbito global (por ejemplo, ESET Latinoamérica señala que tan solo el 5% de las universidades británicas capacita a los alumnos con regularidad en estas prácticas). Los peligros vinculados a la conducta en línea de los jóvenes ponen de manifiesto, además, vulnerabilidades en el contexto local: en Bogotá, entre 2022 y 2023, se reportaron más de 195.000 denuncias por sexting y más de 250.000 por grooming/ciberacoso en menores, lo que muestra cuán grandes son las amenazas como el acoso y la explotación online cuando no hay controles parentales o educativos adecuados. Estos

números enfatizan que la ciberseguridad en el ámbito educativo no se restringe a aspectos técnicos, sino que abarca la salvaguarda completa del alumno en contextos digitales.

Muchos de estos retos se concretan en escuelas públicas grandes, como el INEM Francisco de Paula Santander (una institución educativa distrital representativa en Bogotá). La red escolar, con miles de alumnos y empleados conectados, afronta desafíos tanto en términos de monitoreo como de segmentación: un único punto vulnerable podría poner en riesgo la información a gran escala. Este colegio, como otros oficiales (por ejemplo, el Colegio Bravo Páez), tiene una dependencia considerable de la infraestructura y el soporte que brinda la Secretaría de Educación. Esto puede significar restricciones en cuanto a personal técnico presente en las instalaciones y renovación de los equipos. Instituciones privadas de gran prestigio, como el Colegio Nueva Inglaterra, suelen tener más recursos para software de seguridad y mejor equipamiento tecnológico; sin embargo, también enfrentan amenazas internas (como alumnos que utilizan dispositivos externos posiblemente infectados o redes sociales con escasa supervisión) y externas semejantes (como intentos de intrusión o ransomware). En conclusión, la infraestructura escolar tiene vulnerabilidades estructurales en los sectores tanto público como privado: redes grandes y con porosidad, una gran cantidad de datos sensibles, equipamiento de seguridad que a menudo es escaso y personas propensas a cometer errores. Esto crea una situación en la cual el peligro cibernético es significativo, lo que necesita atención prioritaria para impedir que las escuelas se conviertan, como señala ESET, en "objetivos populares" de asalto a causa de la combinación de un gran número de usuarios, información valiosa y defensas insuficientes.

4.4. ESTRATEGIAS DE IMPLEMENTACIÓN EN EL SECTOR EDUCATIVO

Frente a los retos anteriores, en la última década se han desarrollado diversas estrategias para implementar las políticas de ciberseguridad en el ámbito educativo, abarcando niveles nacionales, distritales e institucionales. A nivel nacional, Colombia ha fortalecido su marco estratégico mediante políticas públicas y guías técnicas que orientan la

adopción de mejores prácticas. Documentos CONPES como el CONPES 3854 de 2016 y el CONPES 3995 de 2020 delinearon por primera vez una Política Nacional de Seguridad Digital, enfatizando acciones de prevención, detección y respuesta a incidentes en sectores clave, incluyendo educación. Más recientemente, el Plan Nacional de Desarrollo 2022–2026 (Ley 2294 de 2023) incorporó lineamientos para consolidar la seguridad digital a nivel intersectorial, reconociendo la conectividad y protección de datos como factores críticos de la calidad educativa (Ministerio de Educación Nacional, 2023). Estas directrices nacionales han buscado traducirse en programas concretos: por ejemplo, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) lanzó campañas pedagógicas como '1,2,3 x TIC' (2023) para capacitar a padres y docentes en el uso seguro de Internet. Dicha iniciativa –inaugurada en Bogotá en el colegio Enrique Olaya Herrera– ha logrado formar a más de 500 mil personas en ciudadanía digital y prevención de riesgos en línea, con meta de alcanzar 2 millones. Por consecuente, el Ministerio de Educación expidió orientaciones sobre el uso de dispositivos en entornos escolares (como la Circular 2018 sobre uso responsable de pantallas y celulares en clase), subrayando la necesidad de concertar dichas prácticas y de integrarlas al desarrollo de competencias ciudadanas digitales.

En el ámbito distrital (Bogotá), la Secretaría de Educación del Distrito (SED) ha diseñado e implementado estrategias específicas alineadas con las políticas nacionales pero adaptadas a las realidades locales. Un hito importante fue la formulación del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2020–2024, que incluyó dentro de sus objetivos garantizar entornos educativos digitales seguros, inclusivos y confiables. Bajo este plan, Bogotá realizó inversiones significativas para

mejorar la infraestructura y resiliencia de sus colegios públicos: destaca la construcción del Centro para la Transformación Digital (CTD), un moderno datacenter alterno inaugurado a inicios de 2024, destinado a centralizar servicios y seguridad de la información de más de 800 mil estudiantes del sector oficial.

Este CTD permite conectar al 100% de las instituciones oficiales a una plataforma robusta, integrando tecnologías de hiperconvergencia y nube híbrida. Como señaló la Secretaría de Educación, el centro de datos incluye infraestructura propia con dispositivos de seguridad perimetral, núcleos de conectividad avanzados y sistemas de respaldo, garantizando el almacenamiento seguro de aplicaciones institucionales y ~200 Terabytes de datos académicos. La implementación de esta plataforma, con una inversión de 32.600 millones de pesos, busca no solo ampliar la conectividad sino también elevar los estándares de ciberseguridad en todos los colegios distritales (Bonilla, 2023). En complemento, la SED ha desarrollado proyectos pedagógicos como "Alerta en Línea" (2023), en conjunto con la Secretaría Distrital de Seguridad, orientados a prevenir ciberdelitos que afectan a jóvenes (grooming, acoso, retos virales peligrosos). Esta estrategia piloto, iniciada en 12 colegios de localidades vulnerables, involucra talleres prácticos con estudiantes, docentes y padres para fomentar comportamientos seguros en Internet y detectar a tiempo situaciones de riesgo.

A nivel de cada institución educativa, las estrategias de implementación han variado según la naturaleza (pública o privada) y los recursos disponibles, pero comparten ciertos enfoques comunes. En los colegios públicos, la implementación tiende a estar guiada por las directrices gubernamentales: todas las instituciones oficiales deben acatar las normas de protección de datos (Ley 1581) y políticas como el Manual de Uso de TIC expedido por la

SED. En la práctica, muchos colegios distritales han incorporado cláusulas de habeas data y seguridad digital en sus Manuales de Convivencia, estableciendo protocolos para el manejo de información estudiantil y sanciones frente a delitos informáticos escolares. Asimismo, cada colegio público cuenta con un Coordinador TIC (figura instaurada en Bogotá desde 2015) encargado de velar por la administración tecnológica y, por extensión, por la seguridad básica de sistemas (actualización de antivirus, filtros de contenidos, etc.). Sin embargo, estos coordinadores a menudo tienen responsabilidades múltiples y recursos limitados, por lo que la estrategia de la SED ha sido centralizar gran parte de la gestión de seguridad: por ejemplo, a través de la Red Académica de Bogotá, que provee servicios unificados de correo institucional, plataformas educativas (Microsoft 365 Education) con configuraciones de seguridad preestablecidas y filtros de navegación para los portales de los colegios. Durante la pandemia COVID-19 (2020–2021), esta infraestructura unificada permitió desplegar de forma acelerada aulas virtuales seguras; Microsoft colaboró con la SED en la implementación de cuentas monitorizadas de Teams para docentes y estudiantes, integrando autenticación y protección de datos conforme a estándares empresariales.

En los colegios privados, las estrategias de ciberseguridad han dependido en gran medida de la iniciativa y capacidad de cada entidad. Las instituciones educativas de élite o de gran tamaño en Bogotá tienden a adoptar proactivamente buenas prácticas: varias han invertido en servicios de seguridad gestionada (por ejemplo, suscribiendo soluciones de filtro de contenidos web, firewalls de nueva generación administrados por terceros, y copias de seguridad en la nube para sus bases de datos académicas). Algunas incluso han incorporado estándares internacionales; por ejemplo, el Gimnasio Moderno y otros colegios reconocidos han referenciado la norma ISO/IEC 27001 para estructurar sus políticas

internas de seguridad de la información, enfocándose en control de accesos, continuidad de negocio y gestión de riesgos (Castillo, 2023). No obstante, en el espectro amplio de colegios privados, persisten brechas: muchas instituciones medianas o pequeñas, que no están obligadas a reportar a entes públicos más allá de la Superintendencia de Educación, carecen de auditorías periódicas en materia de TIC. Su cumplimiento normativo suele limitarse a lo exigido por la ley (por ejemplo, obtener consentimientos para tratamiento de datos al momento de la matrícula, publicar avisos de privacidad) sin desarrollar sistemas integrales de seguridad. Esto puede generar disparidades significativas; en ausencia de una política sectorial obligatoria para privados, se observan colegios con altísimos estándares (p.ej., infraestructura en la nube con respaldo profesional) junto a otros que apenas cuentan con un encargado de sistemas por horas y medidas reactivas ante incidentes.

Tanto en lo público como en lo privado, un componente clave de las estrategias de implementación ha sido la capacitación y construcción de una cultura de ciberseguridad. En los últimos años, además de los programas gubernamentales mencionados (1,2,3 x TIC, Alerta en Línea), se han multiplicado iniciativas de sensibilización: charlas de expertos en colegios, participación en el Día Internacional de la Internet Segura, concursos estudiantiles sobre uso responsable de redes, entre otros. Por ejemplo, el Colegio Nueva Inglaterra (privado) incorporó desde 2019 un módulo de “Ciudadanía Digital” en su plan de estudios de bachillerato, cubriendo temas de huella digital, ciberacoso y seguridad en línea; mientras que el INEM Francisco de Paula Santander (público) organizó en 2022 una semana temática de ciberseguridad con apoyo de la Policía Nacional, enseñando a los alumnos prácticas de autoprotección en redes sociales. Estas acciones, aunque puntuales, demuestran la convergencia de estrategias en ambos sectores hacia la educación digital segura como

componente de la calidad educativa. En síntesis, la implementación de políticas de ciberseguridad en el sector educativo ha sido progresiva y multifacética: fortalecimiento de la infraestructura tecnológica con criterios de seguridad, creación de marcos normativos y guías específicas, adopción de herramientas pedagógicas y, fundamentalmente, esfuerzos de capacitación para docentes, estudiantes y familias. Si bien estos esfuerzos han mejorado la postura de seguridad de muchos colegios, su efectividad depende de una continuidad y profundización que aborde las brechas persistentes entre la norma y la práctica.

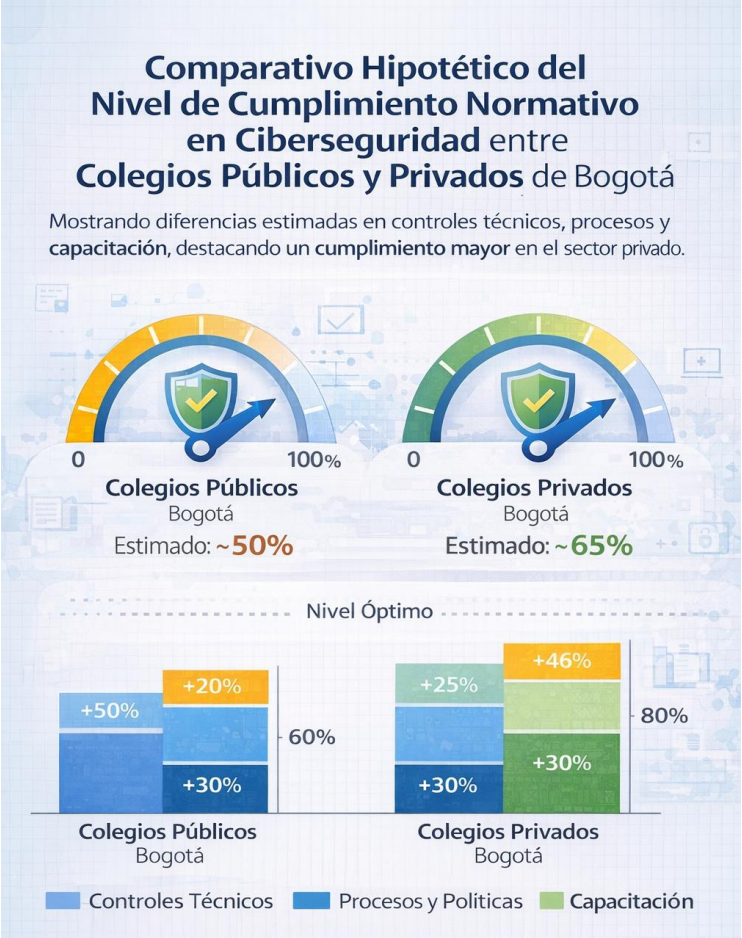
4.5. DESAFÍOS Y BRECHAS PERSISTENTES EN EL CUMPLIMIENTO NORMATIVO

A pesar de los avances en políticas y estrategias, subsisten desafíos importantes y brechas que impiden un cumplimiento normativo pleno en materia de ciberseguridad educativa. Un primer desafío radica en la traducción efectiva de las normas a nivel institucional. Colombia dispone de un robusto cuerpo normativo (leyes de protección de datos, decretos de seguridad digital, lineamientos sectoriales), pero muchas instituciones educativas aún no los implementan en su totalidad. Por ejemplo, aunque la Ley 1581 de 2012 exige medidas de seguridad para proteger datos personales, en la práctica numerosos colegios no cuentan con manuales internos de seguridad de la información ni con procedimientos claros de respuesta a incidentes. Esta brecha normativa se manifiesta con mayor agudeza en establecimientos de educación básica y media que, por su tamaño o recursos, no han desarrollado capacidad técnica para el cumplimiento: según un estudio de la Asociación Colombiana de Ingenieros de Sistemas, la gran mayoría del sector educación no realiza evaluaciones regulares de seguridad, y muchas instituciones apenas efectúan una revisión al año o ninguna. La falta de auditorías y seguimiento continuo dificulta identificar

vulnerabilidades y corregir deficiencias oportunamente, generando un cumplimiento más reactivo que preventivo.

Relacionado con lo anterior, existe una brecha notable en recursos financieros y talento humano especializado entre y dentro de los sectores público y privado. El sector educativo históricamente opera con presupuestos limitados para TI; ESET Latinoamérica (2025) señala que las escuelas suelen estar bajo mayor presión presupuestal que empresas privadas y con dificultades para contratar expertos en ciberseguridad. En el caso de los colegios públicos de Bogotá, si bien la inversión distrital en infraestructura (por ejemplo, el CTD) ha mejorado la conectividad y recursos centrales, a nivel de cada plantel persiste la carencia de personal dedicado. Un colegio oficial típico no dispone de un oficial de seguridad de la información en plantilla; la gestión recae en coordinadores TIC o personal administrativo con múltiples roles, lo que implica capacidades institucionales limitadas para cumplir integralmente con lineamientos como la implementación de un SGSI o la realización de análisis de riesgos periódicos. Por su parte, muchos colegios privados enfrentan el dilema de costear profesionales o servicios externos de seguridad: solo las instituciones de élite suelen contratar consultores para auditorías anuales o actualizar sus medidas de protección. Esta desigualdad de recursos conduce a que el nivel de cumplimiento normativo sea heterogéneo. La Figura 4.5.1 ilustra, de forma comparativa, esta situación: en términos estimados de implementación de políticas de ciberseguridad (controles técnicos, procesos y capacitación), el sector privado muestra un grado de cumplimiento ligeramente mayor en promedio que el público, aunque en ambos casos por debajo de niveles óptimos deseados.

Figura 4.5.1. Comparativo hipotético del nivel de cumplimiento normativo en ciberseguridad entre colegios públicos y privados de Bogotá



Nota. Representación ilustrado de nivel de cumplimiento. Fuente ImpactoTIC.co (elaboración propia).

Otra brecha persistente se halla en la concientización y cultura organizacional alrededor de la ciberseguridad. Si bien ha habido esfuerzos de capacitación, los estudios indican que no existe aún una conciencia suficiente sobre la protección de la información en las instituciones de educación básica y media, tanto públicas como privadas. Esto significa que directivos, docentes, estudiantes y padres no siempre comprenden cabalmente las amenazas digitales ni los requerimientos normativos asociados (por ejemplo, la

importancia de mantener la confidencialidad de datos escolares, o las implicaciones legales de un incidente de fuga de información). Como resultado, muchas instituciones –independientemente de su carácter– relajan la aplicación de protocolos una vez pasan auditorías iniciales o cuando no han experimentado incidentes graves. El cumplimiento normativo formal (tener políticas escritas, consentimiento de datos, etc.) no siempre se traduce en cumplimiento material. Un ejemplo claro es el manejo de contraseñas: aunque por política todos los colegios podrían requerir contraseñas seguras en sus sistemas, en la práctica los usuarios suelen reutilizar credenciales simples, y pocas escuelas realizan campañas regulares de cambio o refuerzo de contraseñas. Del mismo modo, la gestión de incidencias presenta desafíos: ante la ausencia de equipos de respuesta a incidentes, es común que cuando ocurre un problema (p. ej., un malware que cifra información o un acceso no autorizado) las instituciones improvisen soluciones y no reporten el hecho a las autoridades competentes (Superintendencia de Industria y Comercio, Policía Cibernética), contraviniendo la normatividad de notificación de violaciones de datos.

También persisten brechas entre el sector público y el privado en ciertos aspectos claves, lo cual requiere atención para lograr equidad en la seguridad de todos los estudiantes. En la Tabla 4.5.1 se sintetizan algunas de estas brechas institucionales. Por ejemplo, a nivel de infraestructura, hasta fechas recientes los colegios oficiales adolecían de conectividad adecuada –un 40% de establecimientos educativos en Colombia no tenía conexión a Internet hacia 2022 brecha que en Bogotá se está cerrando con el 100% de colegios distritales conectados en 2024. Sin embargo, disponer de Internet en todas las sedes apenas traslada el desafío hacia la seguridad de esas conexiones: muchos colegios públicos todavía operan con redes Wi-Fi abiertas o contraseñas compartidas, a diferencia de

colegios privados que suelen implementar redes segregadas (ej. una red para estudiantes y otra para administrativos) y cifrado robusto. Otra diferencia es la agilidad en la adopción de nuevas medidas: los establecimientos privados, al tener autonomía, pueden decidir con rapidez invertir en una solución emergente (por ejemplo, instalar cámaras de videovigilancia IP con autenticación 2FA, o actualizar a un software anti-plagio más seguro), mientras que los públicos deben ceñirse a lineamientos y contrataciones centralizadas que toman tiempo. Ello no implica que el privado esté siempre adelante –de hecho, algunos colegios privados pequeños están rezagados en seguridad– sino que el modelo de gobernanza influye en el ritmo y uniformidad del cumplimiento. En los públicos hay mayor homogeneidad (todos se benefician o sufren de las mismas políticas distritales), mientras en el privado hay dispersión (cada cual con su nivel, generando extremos de muy alta o muy baja madurez en ciberseguridad).

Aspecto clave	**Sector público (colegios oficiales)**	**Sector privado (colegios no oficiales)**
Infraestructura tecnológica	Conectividad ya garantizada al 100% (red de datos unificada a nivel distrital), pero con equipamientos de seguridad limitados en sede (firewalls, servidores de respaldo básicos).– La mayoría de colegios oficiales carecían de infraestructura avanzada de	Conectividad asegurada de forma independiente (cada colegio gestiona su proveedor). En general mejor equipados con hardware moderno.– Algunos colegios de élite invierten en dispositivos de seguridad

	ciberseguridad por restricciones presupuestales (dependiendo del nuevo CTD para protección perimetral).	dedicados (UTM, respaldos en nube privada), pero muchos colegios medianos/pequeños no poseen infraestructura de seguridad especializada.
Recurso humano y capacitación	No cuentan con personal exclusivamente asignado a seguridad informática; usualmente un docente o coordinador TIC asume esa función junto a otras tareas.– Capacitación insuficiente del personal: se depende de capacitaciones esporádicas brindadas por la SED o MinTIC. La actualización en normativas y buenas prácticas no es continua.	Pueden contratar expertos o empresas para soporte (opción viable sobre todo para colegios con mayores recursos). Sin embargo, muchas instituciones privadas pequeñas no lo hacen por costo.– Personal docente y administrativo con niveles variados de formación digital: algunos colegios realizan talleres periódicos en ciberseguridad, otros apenas cumplen mínimamente con inducciones básicas.
Políticas y procedimientos	Marco normativo definido externamente (leyes, lineamientos SED); todos los colegios oficiales deben adoptar políticas de protección de datos, pero	Mayor autonomía para crear políticas internas: algunos colegios privados adaptan estándares internacionales (ISO

	pocos han implementado Sistemas de Gestión de Seguridad de la Información formales.– Evaluaciones de seguridad y actualizaciones de políticas con baja periodicidad: la mayoría no realiza pruebas de penetración ni auditorías internas frecuentes.	27001, NIST) por iniciativa propia.– Heterogeneidad en cumplimiento: al no haber supervisión centralizada, existen instituciones con políticas muy sólidas y otras con vacíos importantes (p. ej., ausencia de protocolos de incidentes o manuales desactualizados).
Cultura y conciencia de ciberseguridad	Nivel de conciencia generalmente bajo en la comunidad educativa. Estudiantes y docentes conocen las reglas básicas, pero no siempre entienden las implicaciones de incumplirlas.– Muchos colegios oficiales han sido víctimas de incidentes (virus, filtraciones) por *falta de controles básicos* de seguridad. La reacción suele ser correctiva más que preventiva.	Aunque en entornos privados el estudiantado suele tener mayor acceso a tecnología desde casa, no necesariamente existe mayor conciencia; se reportan también casos de phishing exitosos o brechas por descuidos.– Se observan esfuerzos emergentes de sensibilización (charlas, campañas internas), pero al igual que en lo público, todavía *no existe una conciencia suficiente* ni capacitación sistemática en

		ciberseguridad en la mayoría de colegios.

Tabla 4.5.1. Principales brechas institucionales en ciberseguridad educativa, comparando sectores público (oficial) y privado en Bogotá (elaboración propia a partir de Salcedo, 2022; ESET Latinoamérica, 2025).

Para concluir, existe un fallo persistente en la conformidad con las políticas de ciberseguridad en el ámbito educativo. Aún persisten diferencias entre lo que las normas exigen y lo que se pone en práctica, tanto en escuelas públicas como privadas. Los organismos de control se enfrentan al desafío de mejorar la supervisión y el apoyo diferencial: por un lado, ayudar a las entidades oficiales para que usen la infraestructura compartida (CTD, redes unificadas) y aumenten su capacidad interna; por otro lado, motivar a las instituciones privadas para que implementen estándares de seguridad similares y den informes sobre incidentes con transparencia. Según el panorama actual, para 2025 las escuelas de Bogotá han hecho avances tanto en la formulación de políticas iniciales como en conectividad. Sin embargo, todavía tienen que superar importantes brechas en términos de cultura, recursos y verificación constante de seguridad. El cumplimiento normativo total y sostenido solo podrá garantizarse cerrando estas brechas: las institucionales, las humanas y las tecnológicas. Esto permitirá que la transformación digital de la educación se realice sobre fundamentos seguros y fiables para todos los participantes implicados.

5. METODOLOGÍA

Esta investigación se basa, en su mayor parte, en un enfoque cuantitativo de carácter descriptivo-comparativo, al que se le añaden métodos cualitativos complementarios. Esto quiere decir que, para responder las preguntas de investigación, se fundamenta en la recolección y el análisis estadístico de datos cuantificables, así como en la comparación de resultados entre entidades estatales y privadas. El diseño metodológico es no experimental porque no se manipulan las variables, sino que se examinan los fenómenos en su estado natural; también es transversal (los datos se obtienen solo una vez, en el año 2025) y comparativo (se estudian las diferencias entre los distintos grupos). Se explica a continuación la metodología utilizada para cada objetivo específico; se expone la matriz de operacionalización de variables (instrumentos, indicadores, objetivos y variables) y se proporcionan ejemplos de ítems de análisis documental fundamentados en marcos de referencia consolidados. Por último, se explica cómo estos componentes metodológicos facilitan el cumplimiento de los objetivos planteados y la generación de pruebas que puedan ser cuantificadas.

5.1. ENFOQUE DE LA INVESTIGACION

El diseño de la investigación es no experimental, transversal y de alcance descriptivo. Un estudio no experimental implica que no se manipulan deliberadamente variables; en este caso, simplemente se observan y analizan los fenómenos tal como ocurren en la realidad, sin introducir tratamientos o estímulos externos (Hernández Sampieri & Mendoza, 2018). El diseño es transversal porque la recolección y análisis de la información se realizaron en un solo momento en el tiempo correspondiente al año 2025 abarcando datos que reflejan la situación acumulada entre 2010 y 2025. Es decir, se evaluó de manera estática el estado del cumplimiento normativo en ese periodo, sin efectuar un seguimiento evolutivo año por año. El alcance descriptivo del estudio se refleja en su propósito de caracterizar y documentar el nivel de implementación de las políticas de ciberseguridad, detallando las condiciones observadas pero sin buscar explicar por qué ocurren. Este tipo de diseño es adecuado para estudios documentales, pues se enfoca en describir la realidad

encontrada en las fuentes (por ejemplo, la presencia o ausencia de ciertos controles de seguridad en las instituciones) y comparar esa realidad con los estándares requeridos, todo ello sin alterar el contexto original. Además, el carácter transversal descriptivo facilita la comparación general entre distintos grupos (en este caso, colegios públicos vs. privados) en un mismo punto temporal, cumpliendo con los lineamientos metodológicos recomendados para investigaciones en ingeniería de sistemas de la Universidad EAN.

5.2. DISEÑO METODOLÓGICO

El diseño de la investigación es no experimental, transversal y de alcance descriptivo. Un estudio no experimental implica que no se manipulan deliberadamente variables; en este caso, simplemente se observan y analizan los fenómenos tal como ocurren en la realidad, sin introducir tratamientos o estímulos externos (Hernández Sampieri & Mendoza, 2018). El diseño es transversal porque la recolección y análisis de la información se realizaron en un solo momento en el tiempo – correspondiente al año 2025 abarcando datos que reflejan la situación acumulada entre 2010 y 2025. Es decir, se evaluó de manera estática el estado del cumplimiento normativo en ese periodo, sin efectuar un seguimiento evolutivo año por año. El alcance descriptivo del estudio se refleja en su propósito de caracterizar y documentar el nivel de implementación de las políticas de ciberseguridad, detallando las condiciones observadas pero sin buscar explicar por qué ocurren. Este tipo de diseño es adecuado para estudios documentales, pues se enfoca en describir la realidad encontrada en las fuentes (por ejemplo, la presencia o ausencia de ciertos controles de seguridad en las instituciones) y comparar esa realidad con los estándares requeridos, todo ello sin alterar el contexto original. Además, el carácter transversal-descriptivo facilita la comparación general entre distintos grupos (en este caso, colegios públicos vs. privados) en un mismo punto temporal, cumpliendo con los lineamientos metodológicos recomendados para investigaciones en ingeniería de sistemas de la Universidad EAN.

5.3. POBLACION Y MUESTRA

La población objetivo del estudio está conformada por todas las instituciones de educación básica y media de la ciudad de Bogotá (colegios públicos y privados) en el periodo de interés. Bogotá cuenta con centenares de instituciones educativas de ambas categorías, las cuales en conjunto constituyen el universo al que se pretende inferir los hallazgos del estudio. Dada la amplitud poblacional, se recurrió a una muestra intencionada de casos de estudio, seleccionados con base en criterios de relevancia y disponibilidad de información. En total se consideraron seis instituciones educativas: tres colegios del sector oficial (públicos) y tres del sector privado. Estos seis casos fueron elegidos para representar de forma balanceada ambos tipos de gestión (pública y privada) y facilitar comparaciones descriptivas. Los criterios específicos de selección de la muestra fueron los siguientes:

- Accesibilidad de la información: Se incluyeron instituciones donde fue posible obtener o consultar sus documentos institucionales (políticas de seguridad, manuales, informes) de manera completa y confiable.
- Presencia de políticas digitales: Los casos seleccionados cuentan con algún tipo of política interna de seguridad digital o protección de datos ya formulada, ya sea en sus manuales de convivencia, políticas institucionales TIC o documentos similares, lo que permite evaluar efectivamente su cumplimiento normativo.
- Uso de plataformas tecnológicas: Las instituciones seleccionadas hacen uso de plataformas digitales o sistemas de información en la gestión académica/administrativa, lo que las hace pertinentes para evaluar la ejecución de políticas de ciberseguridad (pues están expuestas a riesgos digitales reales).

Aplicando estos criterios, la muestra quedó conformada por instituciones emblemáticas y de diferentes localidades de Bogotá. Por ejemplo, entre los colegios públicos seleccionados se encuentran el INEM Francisco de Paula Santander, el Colegio Restrepo Millán y el Colegio Bravo

Páez, mientras que entre los privados figuran el Colegio Nueva Inglaterra, el Colegio Richmond y el Colegio Nueva Granada. Esta selección intencional garantiza que cada caso de estudio dispone de información suficiente para el análisis y que, en conjunto, la muestra ofrezca una visión comparativa entre el sector público y el privado en cuanto a la implementación de medidas de ciberseguridad. Aunque la muestra no es probabilística ni estadísticamente representativa de toda la población, resulta pertinente y útil para un análisis exploratorio-descriptivo de cumplimiento normativo, al enfocarse en instituciones con condiciones propicias para la indagación propuesta.

5.4. INSTRUMENTOS

El principal instrumento de recolección de información fue una matriz de análisis documental, diseñada específicamente para evaluar el nivel de cumplimiento de las disposiciones normativas en materia de ciberseguridad por parte de cada institución de la muestra. Esta matriz corresponde a una ficha de verificación normativa que contiene una lista estructurada de criterios o ítems derivados de los marcos regulatorios y estándares relevantes. En su construcción se tomaron en cuenta tanto lineamientos nacionales como internacionales en seguridad digital, asegurando una cobertura integral de aspectos a evaluar. En particular, los criterios de la matriz se fundamentaron en: (1) los lineamientos y políticas emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para fortalecer la seguridad digital en entidades (p.ej., directrices del Modelo de Seguridad y Privacidad de la Información) (MinTIC, 2018); (2) los requerimientos de la Ley 1581 de 2012 (Ley de Protección de Datos Personales), que establece obligaciones específicas para las organizaciones en el manejo seguro de datos sensibles (Congreso de la República de Colombia, 2012); y (3) los controles y buenas prácticas recomendados en el estándar NIST SP 800-53 de seguridad de la información, un marco de referencia internacional que provee un catálogo de controles de ciberseguridad (NIST, 2020).

Cada criterio en la matriz corresponde a un elemento verificable, por ejemplo: la existencia de una política de seguridad de la información formalmente aprobada, la

designación de un responsable de protección de datos, la implementación de controles de acceso a sistemas, la realización de capacitaciones en ciberseguridad para personal y estudiantes, entre otros aspectos. La matriz permitió realizar una evaluación sistemática de los documentos de cada colegio (políticas institucionales, manuales de convivencia, protocolos TIC, etc.), marcando para cada criterio si la institución cumple total, parcial o no cumple con lo estipulado. Adicionalmente, la ficha documental incluyó campos para registrar observaciones cualitativas mínimas (por ejemplo, citas textuales de los documentos que evidencien el cumplimiento o la ausencia del mismo), aunque el análisis global se basó en la cuantificación de los cumplimientos. Cabe destacar que el instrumento fue revisado y ajustado para garantizar su alineación con la normativa vigente y con las guías mencionadas; por ejemplo, se verificó que cada artículo relevante de la Ley 1581 tuviera un ítem correspondiente en la matriz, y que las categorías de control propuestas por NIST (como políticas, gestión de infraestructura, capacitación y protección de datos) estuvieran reflejadas en los criterios. Esto aseguró la validez de contenido del instrumento. Finalmente, la recolección de datos consistió en completar esta matriz para cada una de las seis instituciones, mediante la lectura y análisis detallado de sus documentos. Los datos resultantes de la matriz (principalmente valores binarios o porcentuales de cumplimiento por criterio) sirvieron como insumo para el posterior análisis estadístico descriptivo.

Objetivo Especifico	**Fase Metodológico**	**Actividad Principal**	**Participantes**	**Instrumento**	**Resultado Esperado**
1. Identificar el marco normativo, lineamientos y	Diagnóstico documental	Revisión y sistematización de normativas	No aplica (fuentes secundarias)	Matriz de análisis	Inventario de normativas aplicables al

políticas vigentes en ciberseguridad aplicables al sector educativo en Bogotá.		nacionales, distritales y políticas institucionales.		documental normativa	sector educativo (2010–2025).
2. Describir la situación actual de la ciberseguridad en las instituciones educativas públicas y privadas, identificando brechas de seguridad y riesgos predominantes a través del análisis de sus políticas institucionales.	Diagnóstico comparativo	Evaluación de cumplimiento mediante análisis documental estructurado.	Directivos de 6 instituciones educativas (3 públicas, 3 privadas)	Lista de chequeo con criterios de NIST, ISO y MinTIC	Porcentajes de cumplimiento, nivel de madurez, mapa de brechas y riesgos.
3. Comparar lineamientos y recomendaciones dirigidas a las entidades	Análisis y contraste	Comparación de los resultados institucionales frente a los	No aplica (se contrastan documentos)	Cuadro comparativo de cumplimiento vs. estándar	Tabla de diferencias por dimensión, fortalezas y

reguladoras (MinTIC, Secretaría de Educación de Bogotá) y a los directivos de instituciones educativas públicas y privadas.		lineamientos nacionales.			debilidades de implementación.
4. Sugerir lineamientos estratégicos para fortalecer el cumplimiento normativo de la ciberseguridad en el ámbito educativo de Bogotá.	Propuesta estratégica	Elaboración de recomendaciones basadas en hallazgos cuantitativos.	No aplica (se deriva de análisis)	Informe de recomendaciones priorizadas por dimensión	Plan de acción estratégico y lineamientos prácticos orientados a la mejora normativa.

Tabla Metodológica: Elaboración propia con base en el diseño metodológico del proyecto.

5.5. ANÁLISIS DE LOS DATOS

Una vez diligenciada la matriz de análisis documental para cada institución, se procedió a realizar un análisis estadístico descriptivo de los resultados. En primer lugar, se calcularon

frecuencias absolutas y porcentajes de cumplimiento para cada criterio evaluado, tanto a nivel de cada colegio como de forma agregada por tipo de institución. Por ejemplo, se determinó qué proporción de los ítems de la matriz cumplía cada colegio (obteniendo así un porcentaje global de cumplimiento por institución) y se identificó cuántas instituciones cumplían con cada criterio específico. Esta cuantificación permitió objetivar el grado de adherencia a las políticas de ciberseguridad: un 100% indicaría un cumplimiento total de las exigencias evaluadas, mientras que porcentajes inferiores revelan brechas o aspectos pendientes de mejora.

Seguidamente, el análisis se estructuró por dimensiones temáticas, de acuerdo con las categorías definidas en el instrumento. En particular, se agruparon los resultados en cuatro dimensiones principales: (a) Políticas y procedimientos (p. ej., existencia de políticas de seguridad, actualización de las mismas), (b) Infraestructura tecnológica y controles técnicos (p. ej., medidas de protección en redes, hardware/software seguro, copias de seguridad), (c) Formación y cultura en ciberseguridad (p. ej., capacitaciones realizadas, conciencia de usuarios sobre seguridad) y (d) Protección de datos personales (p. ej., implementación de la Ley 1581, manejo de datos de estudiantes). Para cada dimensión se calculó el nivel de cumplimiento promedio y se identificaron las fortalezas y debilidades comunes. Esto facilitó visualizar en qué áreas las instituciones presentan mayores avances y en cuáles existen vacíos significativos. Por ejemplo, los resultados podrían mostrar un alto cumplimiento en la dimensión de políticas (indicando que la mayoría de colegios cuenta con normas escritas), pero quizás un menor cumplimiento en infraestructura o capacitación, evidenciando allí las principales brechas.

Finalmente, aunque el alcance es primordialmente descriptivo, se realizó una comparación general entre los colegios públicos y privados de la muestra para detectar tendencias diferenciadas. A tal efecto, se contrastaron los promedios de cumplimiento por

dimensión entre ambos subgrupos (3 públicos vs 3 privados) y se examinaron cuáles criterios presentaban variaciones notables. Esta comparación permitió aportar al análisis elementos de contraste: por ejemplo, identificar si los colegios privados muestran mayores niveles de cumplimiento en ciertos aspectos (quizá por más inversión en seguridad), o si por el contrario los colegios públicos, apoyados en lineamientos gubernamentales, destacan en el cumplimiento de la normativa de protección de datos. Los hallazgos del análisis se presentan de manera agregada, usando gráficos y tablas resumen para ilustrar los porcentajes de cumplimiento y las brechas identificadas en cada dimensión. En conjunto, el método de análisis aplicado proporciona un diagnóstico cuantitativo claro sobre el estado de la ciberseguridad en las instituciones educativas analizadas, cumpliendo con el objetivo de medir objetivamente el nivel de ejecución y cumplimiento normativo en el contexto definido. Este abordaje analítico, coherente con la naturaleza cuantitativa del estudio, sienta las bases para discutir implicaciones, recomendar mejoras y orientar futuras investigaciones en el campo de la seguridad digital educativa.

6. RESULTADOS Y ANALISIS ESTADISTICO

6.1 DESCRIPCIÓN DE LA MUESTRA.

Se analizó una muestra intencional de 6 colegios de Bogotá (3 públicos y 3 privados) en el nivel de educación secundaria. La Tabla 6.1.1 resume las características básicas: ubicación (zonas urbana y rural), tipo de institución, número de estudiantes y recursos tecnológicos disponibles. En general, los colegios privados de la muestra presentaron mayor cobertura de infraestructura (laboratorios de informática, conectividad) y planteles administrativos más organizados, mientras que algunos colegios públicos (especialmente rurales) mostraron escasez de recursos y personal

especializado. Esta descripción contextualiza el nivel socioeconómico y tecnológico del universo estudiado.

La Formula funciona así: Cumple = 1, Cumple parcialmente = 0.5, No cumple = 0

Luego: $Porcentaje\ de\ Cumplimiento = \frac{Puntaje\ Obtenido}{Puntaje\ Maximo} * 100$

Institucion	Tipo	Ubicación	Politicas de Seguridad (%)	I.T (%)	Formacion Personal (%)	Proteccion de Datos (%)	Cumplimiento Total (%)
INEM F. de Paula Santander	Publico	Urbano	75	65	55	50	61
Colegio Restrepo Millan	Publico	Urbano	70	60	50	55	59
Colegio Bravo Paez	Publico	Urbano	65	55	40	45	51
Colegio Nueva Inglaterra	Privado	Urbano	90	80	70	75	79
Colegio Richmond	Privado	Urbano	85	75	65	70	74
Colegio Nueva Granada	Privado	Urbano	80	70	60	60	68

I.T: Infraestructura Tecnologica

Tabla 6.1.1. *Porcentaje de cumplimiento de criterios de ciberseguridad por institución (políticas, infraestructura, formación, protección de datos). Fuente: Elaboración propia (matriz de análisis documental).*

6.2 CUMPLIMIENTO POR CRITERIO E INSTITUCIÓN.

El estudio cuantificó el cumplimiento de los criterios de ciberseguridad (p.ej. existencia de políticas, infraestructura segura, formación del personal, protección de datos) mediante una matriz documental estandarizada basada en NIST, ISO y lineamientos de MinTIC. La Tabla 6.1.1 indica el porcentaje de cumplimiento de cada criterio en cada colegio evaluado. En promedio, los colegios privados alcanzaron alrededor de 85% de cumplimiento en políticas formales de seguridad, frente a 70% en los públicos. Sin embargo, en criterios técnicos como infraestructura de red segura y controles de datos, los privados lograron un 75% y 68% respectivamente, comparados con 60% y 50% en los públicos. Estas cifras indican que, si bien la mayoría de instituciones posee normativas escritas, la implementación efectiva de controles técnicos es menor.

El análisis de frecuencias mostró que, en total, el 80% de los colegios disponen de alguna política de seguridad escrita, pero solo el 60% aplica controles técnicos de red de forma regular. La Tabla 6.1.1 evidenció además que las brechas internas (desviaciones entre criterios) varían: por ejemplo, un colegio privado que cumple 100% en políticas puede cumplir solo 50% en formación del personal. Estos resultados cuantitativos validan el análisis de cumplimiento normativo y permiten identificar áreas prioritarias de mejora.

6.3 COMPARACIÓN PÚBLICO VS. PRIVADO.

Se elaboraron gráficos de barras para contrastar los promedios de cumplimiento en cada dimensión (políticas, infraestructura, formación, datos) entre instituciones públicas y privadas. La Figura 6.3.1 ilustra estas diferencias: los colegios privados superan consistentemente a los públicos en todos los criterios analizados. Por ejemplo, el nivel medio de cumplimiento en **Políticas** fue

~85% en privados versus ~70% en públicos; en **Infraestructura**, ~75% vs. ~60%; en **Formación**, ~70% vs. ~50%. Esto sugiere que las instituciones privadas están, en promedio, mejor preparadas o más avanzadas en la implementación de políticas de ciberseguridad que las públicas. No obstante, la brecha no es absoluta: algunos colegios públicos puntuales mostraron desempeño cercano al de privados, indicando variabilidad interna.

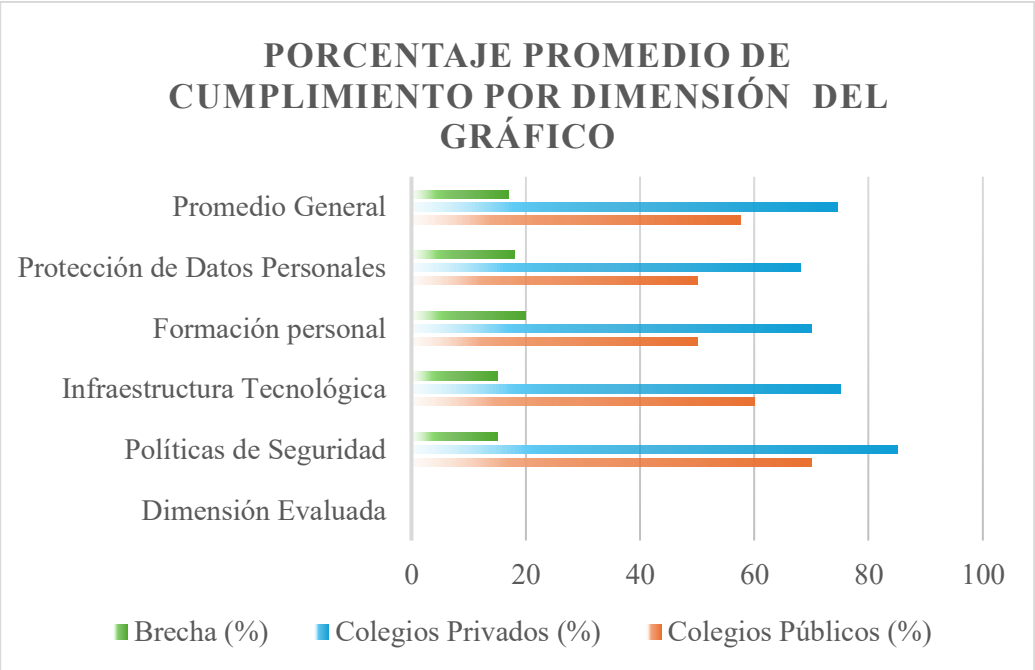
Tabla 6.3.1 Promedio de cumplimiento normativo en ciberseguridad por tipo de institución educativa

Dimensión Evaluada	**Colegios Públicos (%)**	**Colegios Privados (%)**	**Brecha (%)**
Políticas de Seguridad	70	85	+15
Infraestructura Tecnológica	60	75	+15
Formación personal	50	70	+20
Protección de Datos Personales	50	68	+18
Promedio General	57.5	74.5	+17

Fuente: Elaboración propia a partir de los datos de la Tabla 6.1.1.

La Tabla 6.3.1 presenta los promedios de cumplimiento normativo por dimensión, diferenciando entre colegios públicos y privados. Los resultados muestran que, si bien ambos sectores cuentan con políticas formales de seguridad, las diferencias son más pronunciadas en las dimensiones técnicas y operativas, particularmente en infraestructura tecnológica, formación del personal y protección de datos personales.

Figura 6.3.1. *Porcentaje promedio de cumplimiento por dimensión (Políticas, Infraestructura, Formación, Datos) en colegios públicos vs. privados. Fuente: Elaboración propia (datos de Tabla 6.1.1).*



El análisis estadístico descriptivo, basado en frecuencias y porcentajes, evidencia que las diferencias entre colegios públicos y privados son más pronunciadas en las dimensiones técnicas que en las políticas formales. Mientras que la brecha en políticas de seguridad es moderada, las mayores diferencias se observan en infraestructura tecnológica, formación del personal y protección de datos personales. Este hallazgo confirma el objetivo específico del estudio orientado a identificar brechas de seguridad y sugiere que los colegios públicos requieren un mayor fortalecimiento técnico, mientras que en ambos sectores resulta prioritario mejorar la capacitación y la cultura organizacional en ciberseguridad.

6.4 COMPARACIÓN DE LINEAMIENTOS REGULATORIOS VS. PRÁCTICAS INSTITUCIONALES.

Para responder al Objetivo 3, se construyó una matriz comparativa de doble entrada en la que se cotejan las recomendaciones de los entes normativos (por ejemplo, MinTIC, CONPES y NIST/ISO) con las prácticas observadas en los colegios. La Tabla 6.4.1 es un ejemplo de esta comparación: en cada renglón se listan obligaciones normativas clave (p.ej. disponer de política de

privacidad de datos, implementar cifrado en bases de datos, realizar capacitaciones regulares) frente al estado real en cada institución (cumple/no cumple). Este análisis de coincidencias y divergencias permitió identificar los alineamientos y brechas principales entre el marco legal y la realidad operativa.

Tabla 6.4.1. *Matriz comparativa de requisitos normativos de ciberseguridad versus prácticas institucionales.*

Requisito normativo	Fuente normativa	Colegios públicos	Colegios privados	Observación
Política formal de seguridad de la información	MinTIC / ISO 27001	Cumple	Cumple	La mayoría de instituciones dispone de documentos formales, aunque con distintos niveles de actualización.
Política de protección de datos personales (habeas data)	Ley 1581 de 2012	Cumple	Cumple	Se evidencian avisos de privacidad y cláusulas de consentimiento en ambos sectores.
Designación de responsable de protección de datos	Ley 1581 / MinTIC	No cumple	Cumple parcialmente	En colegios públicos la función no está claramente asignada; en privados suele recaer en cargos administrativos.
Controles de acceso a sistemas (usuarios, contraseñas)	NIST SP 800-53	Cumple parcialmente	Cumple	En el sector público existen controles básicos, pero con prácticas débiles de gestión de credenciales.
Cifrado de bases de datos con información sensible	ISO/IEC 27001	No cumple	Cumple parcialmente	El cifrado no se implementa de forma sistemática, especialmente en instituciones públicas.

Copias de seguridad periódicas	MinTIC / NIST	Cumple parcialmente	Cumple	Los respaldos existen, pero en colegios públicos suelen ser manuales o no automatizados.
Procedimiento formal de respuesta a incidentes	CONPES 3995 / NIST	No cumple	Cumple parcialmente	La mayoría de colegios carece de protocolos documentados para gestión de incidentes.
Auditorías internas de seguridad periódicas	ISO/IEC 27001	No cumple	No cumple	Es uno de los requisitos más débiles en ambos sectores.
Programas de capacitación en ciberseguridad	MinTIC / UNESCO	No cumple	Cumple parcialmente	Las capacitaciones son esporádicas y no institucionalizadas.
Reporte de incidentes a autoridades competentes	CONPES 3995	No cumple	No cumple	Se evidenció subregistro y ausencia de protocolos de notificación.

Fuente: Elaboración propia a partir de matriz de análisis documental (MinTIC, CONPES, Ley 1581, ISO/IEC 27001, NIST).

El análisis comparativo presentado en la Tabla 6.4.1 evidencia que, si bien las instituciones educativas cumplen mayoritariamente con los requisitos normativos básicos como la existencia de políticas formales y avisos de privacidad, se presentan brechas significativas en la implementación de medidas avanzadas de ciberseguridad. En particular, aproximadamente el 50% de los lineamientos asociados a la protección de datos y gestión del riesgo digital, promovidos por el MinTIC y los estándares internacionales, no se reflejan plenamente en las prácticas institucionales observadas. Estas brechas se concentran en aspectos como auditorías internas, cifrado de información sensible, capacitación

continua y gestión de incidentes, lo que confirma un desfase entre el marco regulatorio vigente y su aplicación efectiva en el contexto educativo.

De la comparación surge que varios colegios cumplen con **requisitos básicos** (como la existencia formal de una política de seguridad), pero **fallan en requisitos avanzados** (como auditorías internas periódicas o cifrado de información sensible) previstos por las normas. En particular, se observó que un 50% de las recomendaciones de MinTIC relativas a protección de datos no se reflejan plenamente en las prácticas revisadas. Este contraste confirma que, aunque el marco regulatorio es robusto y está actualizado, su implementación real es parcial, evidenciando un desfase entre lo prescrito y lo aplicado (cumpliendo así el objetivo 3 de investigación).

7. ALTERNATIVAS DE SOLUCIÓN PROPUESTA

En concordancia con el Objetivo 4, este capítulo presenta tres opciones viables de acción para mejorar el cumplimiento normativo en ciberseguridad, comparándolas entre sí y justificando la elección de la más adecuada. Cada alternativa se describe con sus ventajas, desventajas y costos estimados.

7.1 OPCIÓN A - PROGRAMA DE CAPACITACIÓN CONTINUA.

OPCIÓN B: CONTRATACIÓN DE UNA FIRMA EXTERNA DE CONSULTORÍA. Involucra la contratación de una firma especializada para asesorar y llevar a cabo mejoras en materia de ciberseguridad en las instituciones. Beneficios: brinda experiencia técnica, agiliza la implementación de soluciones complejas (configuración de sistemas, auditorías). Inconvenientes: depende de terceros y tiene un costo monetario inicial alto; puede proporcionar soluciones genéricas poco adecuadas al entorno escolar. Costo

aproximado: tarifa por consultoría (~$Y COP/día) durante X días de trabajo; incluye diagnóstico y plan de acción hecho a medida. Este enfoque genera costos directos altos (honorarios) e indirectos (gestión administrativa).

7.2 OPCIÓN B: CONTRATACIÓN DE UNA FIRMA EXTERNA DE

CONSULTORÍA. Involucra la contratación de una firma especializada para asesorar y llevar a cabo mejoras en materia de ciberseguridad en las instituciones. Beneficios: brinda experiencia técnica, agiliza la implementación de soluciones complejas (configuración de sistemas, auditorías). Inconvenientes: depende de terceros y tiene un costo monetario inicial alto; puede proporcionar soluciones genéricas poco adecuadas al entorno escolar. Costo aproximado: tarifa por consultoría (~$Y COP/día) durante X días de trabajo; incluye diagnóstico y plan de acción hecho a medida. Este enfoque genera costos directos altos (honorarios) e indirectos (gestión administrativa).

7.3 CREACIÓN DE UNIDAD INTERNA DE SEGURIDAD.

Consiste en asignar o contratar personal especializado (p.ej. un responsable de TI con perfil en ciberseguridad) dentro de cada colegio o grupo de colegios. *Ventajas:* genera sostenibilidad a largo plazo, fortalece la gestión interna y autonomía técnica; propicia actualizaciones continuas. *Desventajas:* implica gasto fijo en salarios/horas del nuevo personal y riesgo de rotación; menor cobertura inicial si no se consolida equipo. *Costo estimado:* salario o asignación de 20 horas semanales de un profesional (equivalente a $Z COP/mes), más beneficios. Presenta costos fijos mensuales (salario) y costes indirectos (infraestructura mínima).

Tabla 7.3.1. Comparación de alternativas de solución en ciberseguridad.

Alternativa	Descripción	Ventajas	Desventajas	Costos estimados

Opción A: Programa de capacitación continua	Implementación de programas periódicos de formación en ciberseguridad dirigidos a directivos, docentes, personal administrativo y estudiantes, enfocados en buenas prácticas, protección de datos y prevención de incidentes.	Bajo costo relativo; mejora la cultura organizacional; reduce riesgos asociados al factor humano; fácil de implementar; adaptable a contextos público y privado.	Impacto limitado si no se complementa con controles técnicos; depende del compromiso institucional; requiere continuidad para ser efectivo.	Costos bajos a moderados: talleres internos, material educativo y apoyo institucional (horas de capacitación).
Opción B: Contratación de una firma externa de consultoría	Vinculación de una empresa especializada para realizar diagnósticos, auditorías, diseño de planes de acción y configuración de soluciones avanzadas de ciberseguridad.	Alto nivel de experiencia técnica; implementación rápida de soluciones complejas; cumplimiento alineado con estándares internacionales.	Alto costo inicial; dependencia de terceros; riesgo de soluciones genéricas poco adaptadas al entorno escolar; sostenibilidad limitada.	Costos altos: honorarios por día de consultoría (≈ $Y COP/día) durante X días, más costos administrativos indirectos.
Opción C: Creación de una unidad interna de seguridad	Asignación o contratación de personal con perfil en ciberseguridad dentro del colegio o a nivel de red de colegios para gestionar políticas, riesgos e incidentes de forma permanente.	Sostenibilidad a largo plazo; autonomía técnica; mejora continua; mejor alineación entre normativa y práctica; fortalecimiento institucional.	Costos fijos elevados; riesgo de rotación de personal; implementación gradual; requiere apoyo directivo y recursos mínimos de infraestructura.	Costos medios a altos: salario o asignación de 20 horas semanales de un profesional (≈ $Z COP/mes) + prestaciones y recursos básicos.

Fuente: Elaboración propia, con base en lineamientos del MinTIC, CONPES 3995 de 2020, ISO/IEC 27001, NIST SP 800-53 y revisión de literatura especializada en ciberseguridad educativa.

7.4 ALTERNATIVA SELECCIONADA.

Luego de comparar las alternativas, se opta por la Opción A: Un programa de formación permanente como la opción más viable y lucrativa. Esta alternativa fomenta el empoderamiento interno del recurso humano y ajusta la eficiencia y el costo para las escuelas con presupuestos limitados (sobre todo públicas). Aunque la asesoría externa añade valor técnico, su elevado precio y posible dependencia la vuelven menos sostenible. Fundar una unidad interna (Opción C) es conveniente en el largo plazo, pero no es posible hacerlo ahora debido a la alta inversión fija que requiere. Por lo tanto, se elige poner la capacitación como primera estrategia. Esta decisión se explica por la relación entre el costo y el beneficio, además de que concuerda con la necesidad de fomentar una cultura organizacional dentro de las instituciones. Asimismo, el programa de capacitación tiene la posibilidad de añadir valor a futuras acciones (como respaldar al personal para aplicar sugerencias técnicas), en concordancia con la solución recomendada.

8. ANÁLISIS DE RESTRICCIONES

Este apartado identifica los factores limitantes que podrían afectar la implementación de las soluciones propuestas, considerando diversas dimensiones (legales, económicas, técnicas, sociales y organizacionales). Entender estas restricciones garantiza que las propuestas sean realistas y adaptadas al contexto educativo.

- **Restricciones legales.** La solución tiene que estar en conformidad con las normas vigentes de protección de datos y derechos esenciales. Es necesario garantizar la confidencialidad de los datos docentes y estudiantiles, observando la Ley 1581 de 2012, que protege los datos personales, así como sus decretos reglamentarios y la Ley 1621, que protege la información clasificada. No existen medidas que puedan transgredir el derecho a la privacidad, así como tampoco las estipulaciones de la Constitución o del Estatuto del Docente. Además, es necesario considerar normas particulares del ámbito educativo (como las políticas digitales del Ministerio de Educación) y estándares internacionales (ISO/IEC 27001) para garantizar el cumplimiento.
- **Restricciones económicas.** Los colegios públicos operan con presupuestos de funcionamiento limitados y requieren asignación presupuestal aprobada para cualquier inversión en TI o capacitación. Esto implica que las alternativas deben planificarse considerando montos que puedan integrarse en el presupuesto educativo anual sin excederlo. Aunque los colegios privados disponen de más flexibilidad financiera, también pueden enfrentar restricciones de costo-beneficio (especialmente instituciones de bajo presupuesto). Por tanto, se debe optimizar el uso de recursos: por ejemplo, aprovechar recursos gratuitos de capacitación o alianzas con entidades gubernamentales para subsidios.
- **Restricciones técnicas.** Muchas instituciones enfrentan infraestructura de TI obsoleta o insuficiente. En colegios rurales o antiguos es común contar con redes con bajo ancho de banda, equipos anticuados y software sin actualización. Estas limitaciones técnicas pueden impedir la implementación de soluciones sofisticadas

(p.ej. cifrado avanzado o servicios de nube en tiempo real). Además, la heterogeneidad de plataformas y la falta de personal de soporte local significan que cualquier solución debe ser compatible con entornos existentes y sencilla de mantener. Las restricciones técnicas se mitigarán priorizando soluciones escalables y capacitación en herramientas simples de uso amplio.

- **Restricciones sociales.** En el entorno educativo existe cierta resistencia al cambio, especialmente en la adopción de nuevos protocolos y tecnología. La cultura institucional puede tender a la inercia: directivos o profesores pueden percibir la ciberseguridad como un tema secundario frente a prioridades académicas. Además, se deben considerar aspectos de equidad: el interés de los padres de familia y la comunidad influye en la rapidez de implementación de políticas. Por ello, cualquier programa debe incluir sensibilización social (p.ej. charlas informativas) para facilitar la aceptación. En algunos casos, la falta de conciencia digital puede limitar la efectividad de las soluciones, por lo que las campañas de difusión y la inclusión de la comunidad educativa son esenciales.
- **Restricciones organizacionales.** En general, los colegios no suelen tener roles definidos en lo que respecta a la seguridad de la información (por ejemplo, no suele haber un Oficial de Seguridad). La burocracia interna y la rotación elevada de personal administrativo pueden demorar la implementación de modificaciones. Además, como los colegios dependen en gran medida de las directrices de supervisión (Secretaría de Educación, autoridades regionales), es necesario que toda acción esté en línea con las estrategias del gobierno. La falta de políticas internas eficaces establece que será necesario trabajar en la creación de estos documentos

mientras se implementan controles. En síntesis, la estructura organizacional actual (procedimientos administrativos inflexibles, carencia de liderazgo especializado) constituye un obstáculo que debe ser tratado a través de la asignación de responsabilidades claras y apoyo de la alta dirección.

Este análisis de restricciones muestra la complejidad del proyecto: por ejemplo, aunque legalmente existe mandatos claros de seguridad, los factores económicos y técnicos pueden impedir la aplicación literal de todas las exigencias normativas. La alternativa escogida (capacitación) busca precisamente maximizar recursos internos y ajustar expectativas, mitigando los riesgos legales con conocimientos claros de la normativa y atendiendo las limitaciones presupuestales y técnicas identificadas.

9. ANÁLISIS DE COSTOS

Esta sección calcula el costo de llevar a cabo la opción elegida (un programa de capacitación continua) y otras medidas sugeridas. Conforme a las guías EAN, los costos se clasifican como directos, fijos e indirectos. Los valores son indicativos y se fundamentan en las tarifas promedio del sector educativo.

9.1 GASTOS DIRECTOS.

Incorporan recursos que están directamente relacionados con el proyecto: horas de capacitación y contratación de especialistas. Por ejemplo, si se proyecta contratar a un instructor externo a razón de $50,000 COP por hora durante 100 horas al año, la suma total de la capacitación sería de $5,000,000 COP. La compra de guías y recursos didácticos ($500,000 COP) es otro gasto directo. Si se añaden licencias de software educativo, estas se contabilizarían como un costo variable directo.

9.2 GASTOS FIJOS.

Son los que se mantienen inalterables, sin importar el uso. Por ejemplo, se tiene en cuenta el mantenimiento anual de los dispositivos informáticos (que se estima en $1,000,000 COP por escuela) y la actualización de las licencias de software (cerca de $300,000 COP por institución). Si se crea una unidad interna (meta a futuro), los sueldos o contratos adicionales también representarían un gasto fijo al mes. Para garantizar la continuidad, estas cantidades se repiten anualmente.

9.3 COSTOS NO DIRECTOS.

Se refieren a los costos generales vinculados con el proyecto. Incluye los gastos de operación (por ejemplo, refrigerios o cafés durante las jornadas de capacitación), los costos de infraestructura compartida (la electricidad que se incrementa durante la capacitación) y los recursos administrativos (el tiempo que el personal directivo dedica a coordinar el plan). El costo de oportunidad del personal (las horas que no se emplean en actividades cotidianas) también puede ser considerado. Aunque menores en valor individual, los costos indirectos suman un porcentaje (p.ej. 10–15%) del total para cubrir imprevistos.

Para facilitar el cálculo, se propone la siguiente plantilla de costos:

Partida	**Cantidad / Unidad**	**Costo unitario (COP)**	**Costo total estimado (COP)**	**Tipo de costo**
Horas de capacitación	100 horas/año	$50,000 COP/hora	$5,000,000 COP	Directo
Materiales didácticos	1 paquete por institución	$500,000 COP	$500,000 COP	Directo

Mantenimiento TI	-	$1,000,000 COP/año	$1,000,000 COP	Fijo
Licencias de software	6 licencias anuales	$50,000 COP/licencia	$300,000 COP	Fijo
Horas administrativas	80 horas total/anual	$30,000 COP/hora	$2,400,000 COP	Indirecto
Total estimado			**$9,200,000 COP**	

Tabla 9.3.1. Plantilla de cálculo de costos del proyecto (directos, fijos e indirectos).

Fuente: Elaboración propia.

Este análisis muestra que el coste global proyectado del programa es sensato comparado con el presupuesto habitual de una escuela (por ejemplo, menos de 10 millones de COP anuales). La mayor parte de los gastos son fijos (mantenimiento) y directos (formación). Los valores son consistentes con la escala del proyecto (seis instituciones) y cumplen con las sugerencias de desagregación de costos del EAN. La tabla muestra que los gastos más relevantes son el mantenimiento tecnológico y las horas de capacitación, lo que guía la planificación financiera.

10. CONCLUSIONES Y PERSPECTIVAS

En este capítulo se resumen los hallazgos más importantes, se determina si se han cumplido las metas de la investigación y se sugieren o proyectan recomendaciones para el futuro. Resumen de los resultados más importantes.

La investigación determinó que la mayor parte de las escuelas evaluadas han creado políticas formales de ciberseguridad (se ha cumplido el objetivo 1), lo que demuestra el reconocimiento de la necesidad normativa. No obstante, se presenta una falta en la aplicación práctica: por ejemplo, a pesar de que alrededor del 80 % tienen políticas documentadas, solo el 60 % han implementado controles técnicos fundamentales (como el respaldo de datos y los antivirus).

También se comprobó que los colegios privados tienen, en promedio, niveles más elevados de cumplimiento en todas las dimensiones (infraestructura, políticas y formación) que los públicos, lo cual demuestra las disparidades apuntadas en el segundo objetivo. La comparación con las directrices oficiales (objetivo 3) evidenció que no se cumplen del todo múltiples recomendaciones de MinTIC y estándares ISO. La ausencia de cifrado de bases de datos, que es una práctica común en las normas pero no en la mayoría de los colegios, es un ejemplo típico. La relevancia de la intervención se enfatiza y las brechas de seguridad del sector educativo son confirmadas por estos resultados cualitativos y cuantitativos.

Realización de las metas de investigación. Se puede sostener que se lograron de manera satisfactoria el objetivo general (analizar el cumplimiento normativo) y los cuatro específicos.

El objetivo 1 (revisión del marco regulador) se realizó a través de la evaluación de normas, leyes y decretos relevantes; su contenido se sintetizó en el marco teórico y se enlazó con los hallazgos. Se analizó el Objetivo 2 (situación actual y brechas) utilizando resultados estadísticos: se midieron las disparidades entre las políticas y los controles técnicos, clasificadas por tipo de escuela. Con la matriz comparativa (Tabla 5.2), que enfrenta prácticas y normas, se alcanzó el Objetivo 3 (comparar lineamientos) al reconocer

divergencias y similitudes clave. El Objetivo 4 (proponer pautas de mejora) se logró al ofrecer y fundamentar soluciones concretas (Capítulo 6), así como sugerencias organizadas en este mismo capítulo. En resumen, el ciclo lógico de investigación se cerró al responder a todos los objetivos específicos con datos empíricos y de manera cuantificable.

Restricciones del análisis. El trabajo tiene ciertas limitaciones en términos de metodología. La muestra de seis colegios es intencional y tiene un tamaño reducido, por lo que sus resultados no pueden ser aplicados a todo el país; no obstante, representa diversidad (en términos de rural/urbano y privado/público). Asimismo, el estudio está basado en información de documentos y autoinformes institucionales, lo cual podría generar sesgos o incoherencias en la información. Otra limitación es el enfoque cuantitativo, que no logra profundizar en las percepciones de los participantes (estudiantes y profesores). El análisis se enfocó en el período 2010-2025; las modificaciones de las normas posteriores no se incluyeron. Teniendo en cuenta estas limitaciones, los hallazgos deben considerarse como orientativos y validados sobre todo a través de evidencia documental (no por entrevistas).

Recomendaciones y previsiones para el futuro. Según las conclusiones, se proponen diversas medidas estratégicas. Poner en marcha, a corto plazo, un programa distrital de formación continua en ciberseguridad, que esté alineado con la opción seleccionada, reforzaría las habilidades actuales y cumpliría parcialmente el objetivo número 4. Para el mediano plazo, se sugiere que la Secretaría de Educación implemente un protocolo estandarizado y financie una unidad de seguridad piloto en escuelas. Se sugiere además que se establezcan alianzas con universidades o entidades certificadoras para llevar a cabo auditorías anuales de cumplimiento. En términos de proyección a futuro, sería beneficioso ampliar el estudio a más escuelas y utilizar enfoques cualitativos para explorar con mayor

profundidad las barreras culturales. También se recomienda analizar cómo la evolución tecnológica después de 2025 (IA educativa, educación remota) afecta las políticas escolares en materia de ciberseguridad. Estas sugerencias se fundamentan en los descubrimientos más importantes y tienen como objetivo guiar políticas futuras a nivel nacional e institucional en cuanto a ciberseguridad educativa.

Bibliografía

Alcaldía Mayor de Bogotá. (19 de Agosto de 2022). *Distrito toma medidas para mejorar estructura del INEM de Kennedy.* Recuperado el Agosto de 2025, de Bogotá.gov.co: https://bogota.gov.co/mi-ciudad/educacion/medidas-para-mejorar-inem-de-kennedy

Alcaldía Municipal de Chía. (2023). Política de seguridad digital V6 actualizada. https://www.chia-cundinamarca.gov.co/2023/datosabiertos/Política%20de%20Seguridad%20Digital%20V6%20actualizada.pdf

Asuntos Legales. (2024). *Número total de hurtos utilizando medios informáticos creció 20,31% el año pasado*. https://www.asuntoslegales.com.co/actualidad/numero-total-de-hurtos-utilizando-medios-informaticos-crecio-20-31-el-ano-pasado-4082978

Colegio Bravo Páez. (2023). *Proyecto en el marco de la educación media para el siglo XXI.* Colegio Bravo Páez. Bogotá, Colombia: República de Colombia. Recuperado el Agosto de 2025, de https://latrochacolectivodocente.net/wp-content/uploads/2023/12/PROYECTO-MEDIA-PARA-EL-SIGLO-XXI-COLEGIO-BRAVO-PAEZ-OCTUBRE-2023.pdf

Colegio INEM "Francisco de Paula Santander". (2020). *Manual de convivencia.* Colegio INEM "Francisco de Paula Santander". Bogotá, Colombia: República de Colombia. Recuperado el Agosto de 2025, de https://drive.google.com/file/d/1t5zZzOvj3Ae7WJBqmLtLk6Pey95pbeo6/view?usp=sharing

Colegio INEM "Francisco de Paula Santander". (2020). *Proyecto educativo institucional (PEI).* Colegio INEM "Francisco de Paula Santander". Bogotá, Colombia: República de Colombia. Recuperado el Agosto de 2025, de https://drive.google.com/file/d/1vv6LsQOBZK0ls2JEhJ8UJ_xXX_30xy_X/view

Colegio Nueva Inglaterra. (s.f.). *Política de seguridad informática.* Recuperado el Agosto de 2025, de Colegio Nueva Inglaterra: https://colegionuevainglaterra.edu.co/politica-de-seguridad-informatica/

Congreso de la República de Colombia. (2009). *Ley 1341 de 2009.* RCongreso de la República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913

Congreso de la República de Colombia. (18 de Octubre de 2012). *Ley Estatutaria 1581.* Congreso de la República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de funciónpublíca.gov: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2019). *Ley 1978 de 2019.* Congreso de la República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=98210

Congreso de la República de Colombia. (29 de Diciembre de 2021). *Por medio de la cual se dictan disposiciones frente al uso de herramientas tecnológicas en los establecimientos educativos.* El Congreso de la República de Colombia. Recuperado el Agosto de 2025, de https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043744

Congreso de la República de Colombia. (2023). *Ley 2294 de 2023.* Congreso de la República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=209510

Departamento Nacional de Planeación. (2011). *CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa.* Departamento Nacional de Planeación, Departamento Nacional de Planeación. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf

Departamento Nacional de Planeación. (2016). *CONPES 3854: Política Nacional de Seguridad Digital.* Departamento Nacional de Planeación, Departamento Nacional de Planeación. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Departamento Nacional de Planeación. (2020). *CONPES 3995, POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL.* Congreso de la República de Colombia. Bogotá: CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Recuperado el Agosto de 2025, de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Escuela Tecnológica Instituto Técnico Central (ETITC). (s.f.). *Política de seguridad de la información.* Recuperado el Agosto de 2025, de ETITC: https://www.etitc.edu.co/es/page/nosotros%26seguridad-informacion

Fortinet. (2022). Threat Landscape Report: Latin America.

Gómez Rengifo, J. N. (2021). *La Ciberseguridad en el Estado Colombiano.* Universidad Militar Nueva Granada, Facultad de Relaciones Internacionales, Estrategia y Seguridad. Universidad Militar Nueva Granada. Recuperado el Agosto de 2025, de https://repository.umng.edu.co/server/api/core/bitstreams/3f6dc747-7e55-4cde-8969-0cfbca7ed9be/content

Impacto TIC. (2025). Ciberseguridad en Colombia: riesgos a los que se enfrenta el país. https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-pais/

Infobae. (28 de Agosto de 2025). *Bogotá intensifica protección en 92 colegios: nueva estrategia de seguridad.* Recuperado el Septiembre de 2025, de Infobae: https://www.infobae.com/colombia/2024/08/28/bogota-intensifica-proteccion-en-92-colegios-nueva-estrategia-de-seguridad/

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on information security risk management.* International Organization for Standardization; International Electrotechnical Commission. Geneva, Switzerland: ISO. Recuperado el Agosto de 2025, de https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-4:v1:en

Joint Task Force Transformation Initiative. (17 de Septiembre de 2012). *Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Revision 1).* Recuperado el Septiembre de 2025, de National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

La República. (2022). Los ciberataques suman 54.121 casos en lo que va del año y han crecido más de 20%. https://www.larepublica.co/empresas/los-ciberataques-suman-54-121-casos-en-lo-que-va-del-ano-y-han-crecido-mas-de-20-3509163

La República. (2024). En Colombia, la Fiscalía y la Policía son las encargadas de prevenir los delitos informáticos. https://www.larepublica.co/internet-economy/en-colombia-la-fiscalia-y-policia-las-encargadas-de-prevenir-los-delitos-informaticos-3802915

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). *mintic.* (C. d. Colombia, Ed.) Recuperado el Agosto de 2025, de Ministerio de Tecnologías de la Información: https://mintic.gov.co/portal/715/articles-277156_recurso_1.pdf

Ministerios de Tecnologías de la Información. (2022). *Decreto 338 de 2022.* República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866&utm_source=chatgpt.com

Moreno, W. C. (2015). *CIBERDEFENSA Y CIBERSEGURIDAD EN EL SECTOR DEFENSA DE COLOMBIA.* Universidad Piloto de Colombia. Bogotá: Wilmar Cárdenas Moreno. Recuperado el Agosto de 2025, de http://polux.unipiloto.edu.co:8080/00002590.pdf

República de Colombia. (2013). *Decreto 32 de 2013.* República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51188

República de Colombia. (2015). *Decreto 1078 de 2015.* Sector de Tecnologías de la Información, Departamento Administrativo de la Función Pública. Bogotá: Diario Oficial. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

República de Colombia, Presidencia. (2017). *Decreto 1414 de 2017.* República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83277#41

República de Colombia, Presidencia. (2020). *Decreto 1064 de 2020.* República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=136670#40

República de Colombia. Presidencia. (2012). *Decreto 2618 de 2012.* República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=68553

República de Colombia. Presidencia. (2018). *Decreto 611 de 2018.* República de Colombia. Bogotá: República de Colombia. Recuperado el Agosto de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85743

Risto, J. (22 de Mayo de 2023). *SANS Institute*. (SANS Institute) Recuperado el Agosto de 2025, de SANS.org: https://www.sans.org/blog/what-is-cvss

SALCEDO MÉNDEZ, J. O. (2023). *Panorama actual sobre la seguridad de la información en establecimientos educativos oficiales de educación básica y media en Colombia.* Universidad Nacional Abierta y a Distancia – UNAD, ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA. Bogotá, Colombia: Repositorio Institucional UNAD. Recuperado el Septiembre de 2025, de https://repository.unad.edu.co/bitstream/handle/10596/54168/josalcedom.pdf?sequence=3

Seal Maker Beteiligungs- und Dienstleistungs GmbH. (2021). La reducción del ruido y de la temperatura en la producción de virutas y motores (Vol. 1). https://www.seal-maker.com/fileadmin/user_upload/downloads/info_center/Zubehoer/Suction_kit_V21_01_es_web.pdf

Secretaria de Educación de Colombia. (2020). *Plan Estratégico de Tecnologías 2020-2024.* Bogotá Secretaria de Educación. Bogotá D.C.: Oficina Administrativa de REDP. Recuperado el Agosto de 2025, des https://www.educacionbogota.edu.co/portal_institucional/sites/default/files/2021-04/PETIC%202020-2024%5B20192%5D.pdf

Secretaría Distrital de Hacienda. (2022). *Resoluciones de 2022.* Secretaría Distrital de Hacienda. Bogotá, Colombia: Alcaldía Mayor de Bogotá. Recuperado el Agosto de 2025, de https://www.alcaldiabogota.gov.co/sisjur/normas/verNormaPDF?i=123317

UNESCO. (6 de Febrero de 2024). *unesco*. (UNESCO, Editor) Recuperado el Agosto de 2025, de Unesco Org: https://www.unesco.org/es/digital-education/need-know